Linksys by Cisco

4-Port Gigabit Security Router with VPN

User Guide

Model: RVS4000

BUSINESS SERIES

cisco

Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.
Copyright © 2008 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

About This Guide

Icon Descriptions

While reading through the User Guide you may see various icons that call attention to specific items. Below is a description of these icons:

NOTE: This check mark indicates that there is a note of interest and is something that you should pay special attention to while using the product.

WARNING: This exclamation point indicates that there is a caution or warning and it is something that could damage your property or product.

WEB: This globe icon indicates a noteworthy website address or e-mail address.

Online Resources

Website addresses in this document are listed without **http://** in front of the address because most current web browsers do not require it. If you use an older web browser, you may have to add **http://** in front of the web address.

Resource	Website
Linksys	www.linksys.com
Linksys International	www.linksys.com/international
Glossary	www.linksys.com/glossary
Network Security	www.linksys.com/security

Copyright and Trademarks

LINKSYS® A Division of Cisco

CISCO

Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2007 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

Open Source

This product may contain material licensed to you under the GNU General Public License or other open-source software licenses. Upon request, open-source software source code is available at cost from Linksys for at least three years from the product purchase date.

WEB: For detailed license terms and additional information visit: **www.linksys.com/gpl**

Table of Contents

Chapter 1: Introduction 1

Chapter 2: Networking and Security Basics 2

An Introduction to LANs . . . 2
The Use of IP Addresses. . . . 2
The Intrusion Prevention System (IPS) . . . 2

Chapter 3: Planning Your Virtual Private Network (VPN) 4

Why do I need a VPN? . . . 4
1) MAC Address Spoofing . . . 4
2) Data Sniffing . . . 4
3) Man in the middle attacks. . . . 4
What is a VPN? . . . 4
VPN Router to VPN Router . . . 5
Computer (using the Linksys VPN client software) to VPN Router . . . 5

Chapter 4: Product Overview 6

Front Panel. . . . 6
Back Panel . . . 6

Chapter 5: Setting Up and Configuring the Router 7

Setup . . . 7
Setup > Summary . . . 7
Setup > WAN . . . 8
Setup > LAN . . . 11
Setup > DMZ . . . 12
Setup > MAC Address Clone . . . 13
Setup > Advanced Routing . . . 13
Setup > Time . . . 14
Setup > IP Mode . . . 14
Firewall . . . 15
Firewall > Basic Settings . . . 15
Firewall > IP Based ACL . . . 15
Firewall > Internet Access Policy . . . 17
Firewall > Single Port Forwarding . . . 18
Firewall > Port Range Forwarding . . . 18
Firewall > Port Range Triggering . . . 19
VPN . . . 19
VPN > Summary . . . 19
VPN > IPSec VPN . . . 20
VPN > VPN Client Accounts . . . 22
VPN > VPN Passthrough . . . 22
QoS . . . 23
QoS > Bandwidth Management . . . 23

QoS > QoS Setup 23
QoS > DSCP Setup 24
Administration 24
Administration > Management 24
Administration > Log 25
Administration > Diagnostics 26
Administration > Backup & Restore 26
Administration > Factory Default 26
Administration > Reboot 26
Administration > Firmware Upgrade 27
IPS 27
IPS > Configuration 27
IPS > P2P/IM 27
IPS > Report 27
IPS > Information 28
L2 Switch 28
L2 > Create VLAN 28
L2 > VLAN Port Setting 29
L2 > VLAN Membership 29
L2 > RADIUS 29
L2 > Port Setting 30
L2 > Statistics 30
L2 > Port Mirroring 30
L2 > RSTP 30
Status 31
Status > Gateway 31
Status > Local Network 31

Appendix A: Troubleshooting 33

Frequently Asked Questions 38

Appendix B: Using Linksys QuickVPN for Windows 2000, XP, or Vista 41

Overview 41
Before You Begin 41
Installing the Linksys QuickVPN Software 41
Installing from the CD-ROM 41
Downloading and Installing from the Internet 41
Using the Linksys QuickVPN Software 42
Version Number of the QuickVPN Client 42
Distributing Certificates to QuickVPN Users 43

Appendix C: Configuring IPSec with a Windows 2000 or XP Computer 44

Introduction 44
Environment 44

How to Establish a Secure IPSec Tunnel 44
Step 1: Create an IPSec Policy 44
Step 2: Build Filter Lists 44
Step 3: Configure Individual Tunnel Rules 46
Step 4: Assign New IPSec Policy. 49
Step 5: Create a Tunnel Through the Web-Based Utility. 49

Appendix D: Gateway-to-Gateway VPN Tunnel 50

Overview. 50
Before You Begin 50
Configuration when the Remote Gateway Uses a Static IP Address 50
Configuration of the RVS4000. 50
Configuration of the RV082 51
Configuration of PC 1 and PC 2 51
Configuration when the Remote Gateway Uses a Dynamic IP Address. 52
Configuration of the RVS4000. 52
Configuration of the RV082 52
Configuration of PC 1 and PC 2 53
Configuration when Both Gateways Use Dynamic IP Addresses 53
Configuration of the RVS4000. 53
Configuration of the RV082 54
Configuration of PC 1 and PC 2 54

Appendix E: Trend Micro ProtectLink Gateway Service 55

Overview. 55
How to Access the Web-Based Utility 55
How to Purchase, Register, or Activate the Service. 55
ProtectLink. 55
How to Use the Service 56
ProtectLink > Web Protection 56
ProtectLink > Email Protection 57
ProtectLink > License 57

Appendix F: Specifications 60

Appendix G: Warranty Information 62

Exclusions and Limitations. 62
Obtaining Warranty Service 62
Technical Support 63

Appendix H: Regulatory Information 64

FCC Statement 64
Safety Notices. 64
Industry Canada Statement 64

Avis d'Industrie Canada 64
User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE) 65

Appendix I: Software License Agreement 69

Software in Linksys Products: 69
Software Licenses: 69
Schedule 1 Linksys Software License Agreement. 69
Schedule 2 70
Schedule 3 73

Appendix J: Contact Information 76

Chapter 1: Introduction

Thank you for choosing the 4-Port Gigabit Security Router with VPN. The Linksys 4-Port Gigabit Security Router with VPN is an advanced Internet-sharing network solution for your small business needs. Like any router, it lets multiple computers in your office share an Internet connection.

The 4-Port Gigabit Security Router with VPN also features a built-in 4-Port full-duplex 10/100/1000 Ethernet switch to connect four PCs directly, or you can connect more hubs and switches to create as big a network as you need.

The Virtual Private Network (VPN) capability creates encrypted "tunnels" through the Internet, allowing up to 5 remote offices and 5 traveling users to securely connect into your office network from off-site. Users connecting through a VPN tunnel are attached to your company's network — with secure access to files, e-mail, and your intranet — just as if they were in the building. You can also use the VPN capability to allow users on your small office network to securely connect out to a corporate network. The QoS features provide consistent voice and video quality throughout your business.

The 4-Port Gigabit Security Router with VPN can serve as a DHCP Server, and has a powerful SPI firewall and Intrusion Prevention System (IPS) to protect your PCs against intruders and most known Internet attacks. It can be configured to filter internal users' access to the Internet, and has IP and MAC address filtering so you can specify exactly who has access to your network. Configuration is a snap with the web browser-based configuration utility.

This user guide will give you all the information you need to connect, set up, and configure your Router.

Chapter 2: Networking and Security Basics

An Introduction to LANs

A Router is a network device that connects two networks together.

The Router connects your local area network (LAN), or the group of PCs in your home or office, to the Internet. The Router processes and regulates the data that travels between these two networks.

The Router's Network Address Translation (NAT) technology protects your network of PCs so users on the Internet cannot "see" your PCs. This is how your LAN remains private. The Router protects your network by inspecting the first packet coming in through the Internet port before delivery to the final destination on one of the Ethernet ports. The Router inspects Internet port services like the web server, ftp server, or other Internet applications, and, if allowed, it will forward the packet to the appropriate PC on the LAN side.

The Use of IP Addresses

IP stands for Internet Protocol. Every device in an IP-based network, including PCs, print servers, and routers, requires an IP address to identify its location, or address, on the network. This applies to both the Internet and LAN connections.

There are two ways of assigning IP addresses to your network devices.

A static IP address is a fixed IP address that you assign manually to a PC or other device on the network. Since a static IP address remains valid until you disable it, static IP addressing ensures that the device assigned it will always have that same IP address until you change it. Static IP addresses are commonly used with network devices such as server PCs or print servers.

If you use the Router to share your cable or DSL Internet connection, contact your ISP to find out if they have assigned a static IP address to your account. If so, you will need that static IP address when configuring the Router. You can get the information from your ISP.

A dynamic IP address is automatically assigned to a device on the network. These IP addresses are called dynamic because they are only temporarily assigned to the PC or other device. After a certain time period, they expire and may change. If a PC logs onto the network (or the Internet) and its dynamic IP address has expired, the DHCP server will assign it a new dynamic IP address.

A DHCP server can either be a designated PC on the network or another network device, such as the Router. By default, the Router's Internet Connection Type is **Obtain an IP automatically** (DHCP).

The PC or network device obtaining an IP address is called the DHCP client. DHCP frees you from having to assign IP addresses manually every time a new user is added to your network.

For DSL users, many ISPs may require you to log on with a user name and password to gain access to the Internet. This is a dedicated, high-speed connection type called Point to Point Protocol over Ethernet (PPPoE). PPPoE is similar to a dial-up connection, but PPPoE does not dial a phone number when establishing a connection. It also will provide the Router with a dynamic IP address to establish a connection to the Internet.

By default, a DHCP server (on the LAN side) is enabled on the Router. If you already have a DHCP server running on your network, you MUST disable one of the two DHCP servers. If you run more than one DHCP server on your network, you will experience network errors, such as conflicting IP addresses. To disable DHCP on the Router, see the Basic Setup section in "Chapter 6: Setting Up and Configuring the Router."

NOTE: Since the Router is a device that connects two networks, it needs two IP addresses—one for the LAN, and one for the Internet. In this User Guide, you'll see references to the "Internet IP address" and the "LAN IP address."

Since the Router uses NAT technology, the only IP address that can be seen from the Internet for your network is the Router's Internet IP address. However, even this Internet IP address can be blocked, so that the Router and network seem invisible to the Internet.

The Intrusion Prevention System (IPS)

IPS is an advanced technology to protect your network from malicious attacks. IPS works together with your SPI Firewall, IP Based Access Control List (ACL), Network Address Port Translation (NAPT), and Virtual Private Network (VPN) to achieve the highest level of security. IPS works by providing real-time detection and prevention as an in-line module in a router.

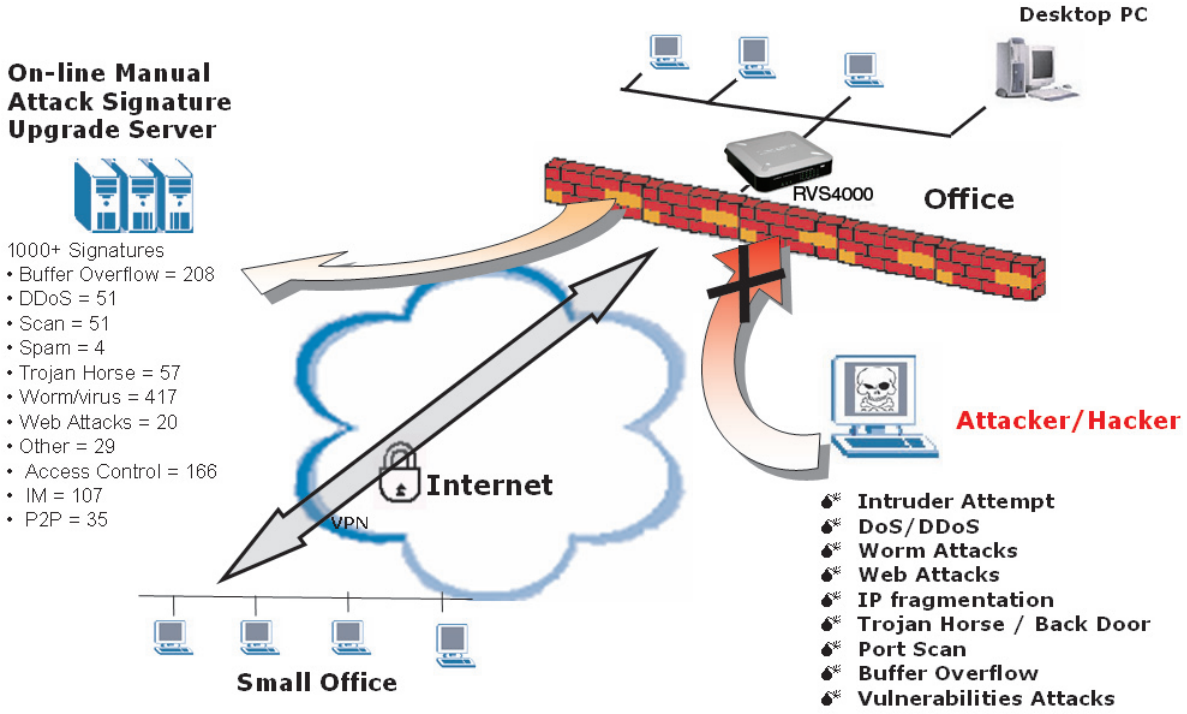
The RVS4000 has hardware-based acceleration for real-time pattern matching for detecting malicious attacks. It actively filters and drops malicious TCP/UDP/ICMP/IGMP packets and can reset TCP connections. This protects your

client PCs and servers running various operating systems including Windows, Linux, and Solaris from network worm attacks. However, this system does not prevent viruses contained in email attachments.

The P2P (peer-to-peer) and IM (instant messaging) control allows the system administrator to prevent network users from using those protocols to communicate with people over the Internet. This helps the administrators to set up company policies on how to use the Internet bandwidth wisely.

The signature file is the heart of the IPS system. It is similar to the Virus definition file on your PC's Anti-Virus software. IPS uses this file to match against packets coming into the Router and performs actions accordingly. The RVS4000 is shipped with a signature file containing 1000+ rules, which cover the following categories: DDoS, Buffer Overflow, Access Control, Scan, Trojan Horse, Misc., P2P, IM, Virus, Worm, and Web Attacks.

Customers are encouraged to update their IPS signature file regularly to prevent any new types of attacks on the Internet.



IPS Scenarios

Chapter 3: Planning Your Virtual Private Network (VPN)

Why do I need a VPN?

Computer networking provides a flexibility not available when using an archaic, paper-based system. With this flexibility, however, comes an increased risk in security. This is why firewalls were first introduced. Firewalls help to protect data inside of a local network. But what do you do once information is sent outside of your local network, when e-mails are sent to their destination, or when you have to connect to your company's network when you are out on the road? How is your data protected?

That is when a VPN can help. VPNs are called Virtual Private Networks because they secure data moving outside of your network as if it were still within that network.

When data is sent out across the Internet from your computer, it is always open to attacks. You may already have a firewall, which will help protect data moving around or held within your network from being corrupted or intercepted by entities outside of your network, but once data moves outside of your network—when you send data to someone via e-mail or communicate with an individual over the Internet—the firewall will no longer protect that data.

At this point, your data becomes open to hackers using a variety of methods to steal not only the data you are transmitting but also your network login and security data. Some of the most common methods are as follows:

1) MAC Address Spoofing

Packets transmitted over a network, either your local network or the Internet, are preceded by a packet header. These packet headers contain both the source and destination information for that packet to transmit efficiently. A hacker can use this information to spoof (or fake) a MAC address allowed on the network. With this spoofed MAC address, the hacker can also intercept information meant for another user.

2) Data Sniffing

Data "sniffing" is a method used by hackers to obtain network data as it travels through unsecured networks, such as the Internet. Tools for just this kind of activity, such as protocol analyzers and network diagnostic tools, are often built into operating systems and allow the data to be viewed in clear text.

3) Man in the middle attacks

Once the hacker has either sniffed or spoofed enough information, he can now perform a "man in the middle" attack. This attack is performed, when data is being transmitted from one network to another, by rerouting the data to a new destination. Even though the data is not received by its intended recipient, it appears that way to the person sending the data.

These are only a few of the methods hackers use and they are always developing more. Without the security of your VPN, your data is constantly open to such attacks as it travels over the Internet. Data travelling over the Internet will often pass through many different servers around the world before reaching its final destination. That's a long way to go for unsecured data and this is when a VPN serves its purpose.

What is a VPN?

A VPN, or Virtual Private Network, is a connection between two endpoints—a VPN Router, for instance—in different networks that allows private data to be sent securely over a shared or public network, such as the Internet. This establishes a private network that can send data securely between these two locations or networks.

This is done by creating a "tunnel". A VPN tunnel connects the two PCs or networks and allows data to be transmitted over the Internet as if it were still within those networks. Not a literal tunnel, it is a connection secured by encrypting the data sent between the two networks.

VPN was created as a cost-effective alternative to using a private, dedicated, leased line for a private network. Using industry standard encryption and authentication techniques—IPSec, short for IP Security—VPN creates a secure connection that, in effect, operates as if you were directly connected to your local network. VPN can be used to create secure networks linking a central office with branch offices, telecommuters, and/or professionals on the road (travelers can connect to a VPN Router using any computer with the Linksys VPN client software.)

There are two basic ways to create a VPN connection:

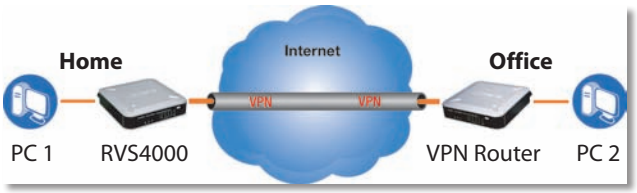
- VPN Router to VPN Router
- Computer (using the Linksys VPN client software) to VPN Router

The VPN Router creates a "tunnel" or channel between two endpoints, so that data transmissions between them are secure. A computer with the Linksys VPN client software can be one of the two endpoints (refer to "Appendix B: Using Linksys QuickVPN for Windows 2000, XP, or Vista"). If you choose not to run the VPN client software, any computer with the built-in IPSec Security Manager (Microsoft 2000 and XP) allows the VPN Router to create a

VPN tunnel using IPSec (refer to "Appendix C: Configuring IPSec between a Windows 2000 or XP PC and the Router"). Other versions of Microsoft operating systems require additional, third-party VPN client software applications that support IPSec to be installed.

VPN Router to VPN Router

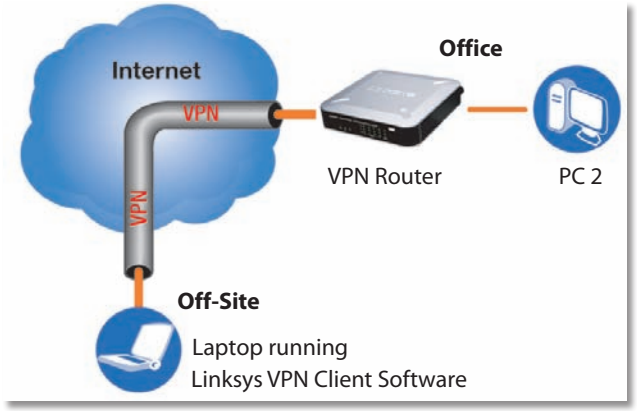
An example of a VPN Router-to-VPN Router VPN would be as follows. At home, a telecommuter uses his VPN Router for his always-on Internet connection. His router is configured with his office's VPN settings. When he connects to his office's router, the two routers create a VPN tunnel, encrypting and decrypting data. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the telecommuter now has a secure connection to the central office's network, as if he were physically connected. For more information, refer to "Appendix D: Configuring a Gateway-to-Gateway IPSec Tunnel."



VPN Router to VPN Router

Computer (using the Linksys VPN client software) to VPN Router

The following is an example of a computer-to-VPN Router VPN. In her hotel room, a traveling businesswoman dials up her ISP. Her notebook computer has the Linksys VPN client software, which is configured with her office's IP address. She accesses the Linksys VPN client software and connects to the VPN Router at the central office. As VPNs utilize the Internet, distance is not a factor. Using the VPN, she now has a secure connection to the central office's network, as if she were physically connected.



Computer to VPN Router

For additional information and instructions about creating your own VPN, please visit Linksys's website at www.linksys.com. You can also refer to "Appendix B: Using Linksys QuickVPN for Windows 2000, XP, or Vista", "Appendix C: Configuring IPSec between a Windows 2000 or XP PC and the Router," and "Appendix D: Configuring a Gateway-to-Gateway IPSec Tunnel."

Chapter 4: Product Overview

Front Panel

The Router's LEDs are located on the front panel of the Router.

Front Panel

- **POWER** (Green) The Power LED lights up when the Router is powered on. If the LED is flashing, the Router is running a diagnostic test.
- **DIAG** (Red) The Diag LED lights up when the system is not ready. The LED goes off when the system is ready. The Diag LED blinks during Firmware upgrades.
- **IPS** (Green/Red) The IPS LED lights up when the IPS function is enabled. If the LED is off, then IPS functions are disabled. If the IPS LED is flashing green, then an external attack has been detected. If the IPS LED is flashing red, an internal attack has been detected.
- **1-4 (ETHERNET)** (Green) For each port, there are three LEDs. If the corresponding LED is continuously lit, the Router is connected to a device at the speed indicated through the corresponding port (1, 2, 3, or 4). If the LED is flashing, the Router is actively sending or receiving data over that port.
- **INTERNET** (Green) The Internet LED lights up the appropriate LED depending upon the speed of the device attached to the Internet port. If the Router is connected to a cable or DSL modem, typically the 10 LED will be the only LED lit up. Flashing indicates activity.

Back Panel

The Router's ports and Reset button are located on the back panel of the Router.

Back Panel

RESET The Reset button can be used in one of two ways:

- If the Router is having problems connecting to the Internet, press the Reset button for just a second with a paper clip or a pencil tip. This is similar to pressing the Reset button on your PC to reboot it.
- If you are experiencing extreme problems with the Router and have tried all other troubleshooting measures, press and hold in the Reset button for 10 seconds. This will restore the factory defaults and clear all of the Router's settings, such as port forwarding or a new password.

INTERNET The Internet port connects to a cable or DSL modem.

1-4 (ETHERNET) The four Ethernet ports connect to network devices, such as PCs, print servers, or additional switches.

POWER The Power port is where you will connect the AC power cable.

Chapter 5: Setting Up and Configuring the Router

The router is configured using the built-in Web-based Utility. To access the Web-based Utility of the Router, open your web browser and enter **http://192.168.1.1** into the *Address* field. Press the **Enter** key and the Login screen will appear.

Address Bar of Web Browser

NOTE: The default IP address is **192.168.1.1**. If the IP address has been changed using DHCP or via the console interface, enter the assigned IP address instead of the default.

The first time you open the web-based utility, enter **admin** (the default username) in the *Username* field and enter **admin** in the *Password* field. Click the **OK** button. You can change the password later from the Administration tab's *Management* screen.

Login Screen

After you log in, the web-based utility starts. The utility's main functions are indicated by eight tabs that appear at the top of each screen: **Setup**, **Firewall**, **VPN**, **QoS**, **Administration**, **IPS**, **L2 Switch**, and **Status**. After you select a tab, a list of that tab's screens is displayed below the tab bar. To perform a specific function, you select a tab, then select the appropriate screen. By default, the Setup tab's *Summary* screen is the first screen displayed following login.

The utility's tabs and screens are described below. For brevity, screen names are listed using the notation: *TabName* > *ScreenName*.

Setup

The Setup tab is used to access all of the Router's basic setup functions. The device can be used in most network settings without changing any of the default values. Some users may need to enter additional information in order to connect to the Internet through an ISP (Internet Service Provider) or broadband (DSL, cable modem) carrier

Setup > Summary

The *Setup* > *Summary* screen displays a read-only summary of the Router's basic information. Clicking on a hyperlink (underlined text) takes you directly to the related page where you can update the information.

Setup > Summary

System Information

Firmware version Displays the Router's current software version.

CPU Displays the Router's CPU type.

System up time Displays the length of time that has elapsed since the Router was last reset.

DRAM Displays the amount of DRAM installed in the Router.

Flash Displays the amount of flash memory installed in the Router.

Port Statistics

This section displays the following color-coded status information on the Router's Ethernet ports:

- **Green** Indicates that the port has a connection.
- **Black** Indicates that the port has no connection.

Network Setting Status

LAN IP Displays the IP address of the Router's LAN interface.

WAN IP Displays the IP address of the Router's WAN interface. If this address was assigned using DHCP, click **DHCP Release** to release the address, or click **DHCP Renew** to renew the address.

Mode Displays the operating mode, **Gateway** or **Router**.

Gateway Displays the Gateway address, which is the IP address of your ISP's server.

DNS 1-2 The IP addresses of the Domain Name System (DNS) server(s) that the Router is using.

DDNS Indicates whether the Dynamic Domain Name System (DDNS) feature is enabled.

DMZ Host Indicates whether the DMZ Hosting feature is enabled.

Firewall Setting Status

DoS (Denial of Service) Indicates whether the DoS Protection feature is enabled to block DoS attacks.

Block WAN Request Indicates whether the Block WAN Request feature is enabled.

Remote Management Indicates whether the Remote Management feature is enabled.

IPSec VPN Setting Status

IPSec VPN Summary Click the **IPSec VPN Summary** hyperlink to display the *VPN* > *Summary* screen.

Tunnel(s) Used Displays the number of VPN tunnels currently being used.

Tunnel(s) Available Displays the number of VPN tunnels that are available.

Log Setting Status

E-mail If this displays *Email cannot be sent because you have not specified an outbound SMTP server address*, then you have not set up the mail server. Click the **E-mail** hyperlink to display the *Administration* > *Log* screen where you can configure the SMTP mail server.

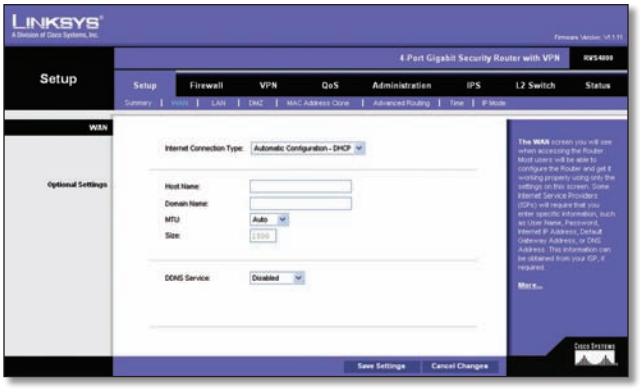
Setup > WAN

Internet Connection Type

The Router supports six types of connections. Each *Setup* > *WAN* screen and available features will differ depending on what kind of connection type you select.

Automatic Configuration - DHCP

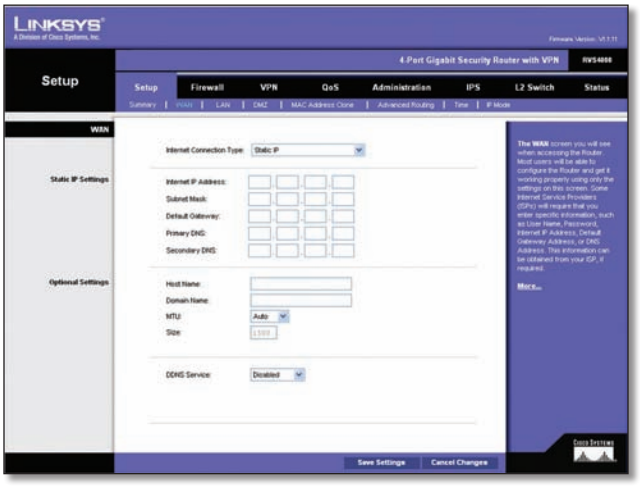
By default, the Router's Configuration Type is set to **Automatic Configuration - DHCP**, and it should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address.



Automatic Configuration - DHCP

Static IP

If your connection uses a permanent IP address to connect to the Internet, then select **Static IP.**



Static IP

Internet IP Address This is the Router's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.

Subnet Mask This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

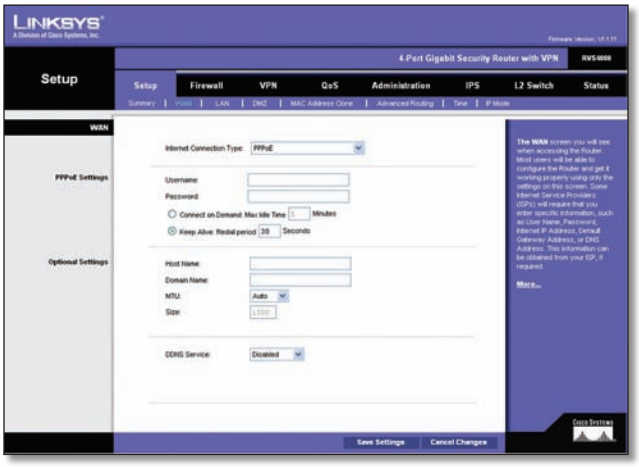
Default Gateway Your ISP will provide you with the Default Gateway Address, which is the ISP server's IP address.

Primary DNS (Required) and Secondary DNS (Optional) Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

When you have finished making changes to the screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes.

PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable PPPoE.



PPPoE

User Name and Password Enter the User Name and Password provided by your ISP.

Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time), and then automatically re-establish the connection as soon as you attempt to access the Internet again. To activate Connect on Demand, select the **Connect on Demand** option and enter in the *Max Idle Time* field the number of minutes of inactivity that must elapse before your Internet connection is terminated automatically.

Keep Alive: Redial period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. In the *Redial Period* field, specify how often you want the Router to check the Internet connection. The default Redial Period is **30** seconds.

When you have finished making changes to the screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes.

PPTP

Point-to-Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe and Israel only.

PPTP

IP Address This is the Router's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.

Subnet Mask This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Default Gateway Your ISP will provide you with the Default Gateway Address.

PPTP Server Enter the IP address of the PPTP server.

User Name and Password Enter the User Name and Password provided by your ISP.

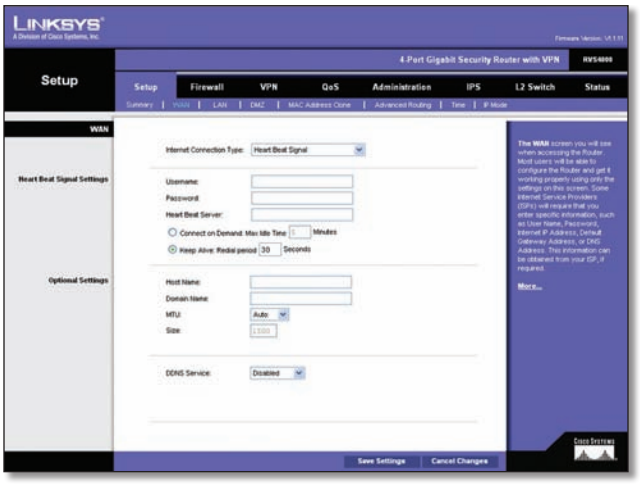
Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time), and then automatically re-establish the connection as soon as you attempt to access the Internet again. To activate Connect on Demand, select the **Connect on Demand** option and enter in the *Max Idle Time* field the number of minutes of inactivity that must elapse before your Internet connection is terminated automatically.

Keep Alive: Redial period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. In the *Redial Period* field, specify how often you want the Router to check the Internet connection. The default Redial Period is **30** seconds.

When you have finished making changes to the screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes.

Heart Beat Signal

Heart Beat Signal is a service used in Australia. Check with your ISP for the necessary setup information.



Heart Beat Signal

User Name and Password Enter the User Name and Password provided by your ISP.

Heart Beat Server Enter the IP address of the Heart Beat server.

Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time), and then automatically re-establish the connection as soon as you attempt to access the Internet again. To activate Connect on Demand, select the **Connect on Demand** option and enter in the *Max Idle Time* field the number of minutes of inactivity that must elapse before your Internet connection is terminated automatically.

Keep Alive: Redial period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. In the *Redial Period* field, specify how often you want the Router to check the Internet connection. The default Redial Period is **30** seconds.

When you have finished making changes to the screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes.

L2TP

Layer 2 Tunneling Protocol (L2TP) is a service that tunnels Point-to-Point Protocol (PPP) across the Internet. It is used mostly in European countries. Check with your ISP for the necessary setup information.

L2TP

IP Address This is the Router's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.

Subnet Mask This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Gateway Your ISP will provide you with the Default Gateway Address.

L2TP Server Enter the IP address of the L2TP server.

User Name and Password Enter the User Name and Password provided by your ISP.

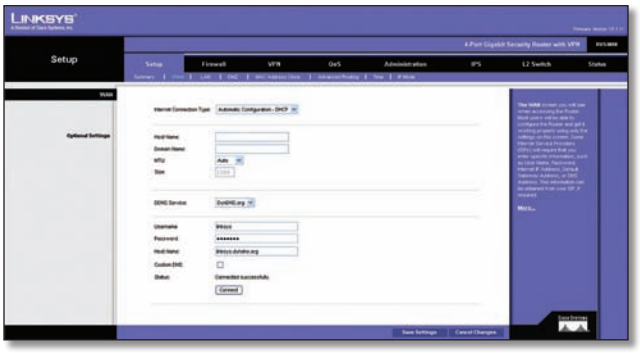
Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time), and then automatically re-establish the connection as soon as you attempt to access the Internet again. To activate Connect on Demand, select the **Connect on Demand** option and enter in the *Max Idle Time* field the number of minutes of inactivity that must elapse before your Internet connection is terminated automatically.

Keep Alive: Redial period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. In the *Redial Period* field, you specify how often you want the Router to check the Internet connection. The default Redial Period is **30** seconds.

When you have finished making changes to the screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes.

Optional Settings (Required by some ISPs)

Some of these settings may be required by your ISP. Verify with your ISP before making any changes.



Optional Settings

Host Name Some ISPs, usually cable ISPs, require a host name as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host name. In most cases, leaving this field blank will work.

Domain Name Some ISPs, usually cable ISPs, require a domain name as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a domain name. In most cases, leaving this field blank will work.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select Manual if you want to manually enter the largest packet size that will be transmitted. To have the Router select the best MTU for your Internet connection, keep the default setting, **Auto**.

Size When Manual is selected in the MTU field, this option is enabled. It is recommended that you set this value within the range of 1200 to 1500, but the value can be defined between 128 and 1500.

DDNS Service DDNS Service is disabled by default. To enable DDNS Service, follow these instructions:

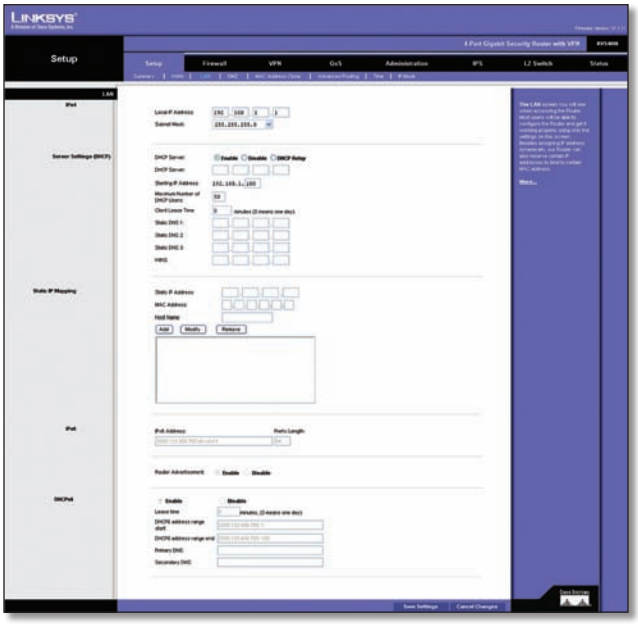
1. Sign up for DDNS Service
   - DynDNS - Sign up for DDNS service at www.dyndns.org, and write down your User Name, Password, and Host Name information.
   - TZO - Sign up for DDNS service at www.tzo.com, and write down your E-mail Address, Password and Domain Name information.
2. Select the DDNS service provider whose service you are using.
3. Configure the following fields:
   - User Name (DynDNS) or E-mail address (TZO).
   - Password
   - Host Name (DynDNS) or Domain name (TZO)
   - Custom DNS (DynDNS)
4. Click **Save Settings**.

The Router will now advise the DDNS Service of your current WAN (Internet) IP address whenever this address changes. If using TZO, you should NOT use the TZO software to perform this "IP address update".

Connect The **Connect** button is displayed when DDNS is enabled. This button is used to contact the DDNS server to manually update your IP address information. The Status area on this screen is also updated.

Setup > LAN

The *Setup* > *LAN* screen allows you to change the Router's local network settings.



Setup > LAN

VLAN Select the VLAN for the DHCP server from the drop-down menu.

NOTE: This option appears only if you have created at least one VLAN from the *L2 Switch* > *Create VLAN* screen.

IPv4

The Router's Local IP Address and Subnet Mask are shown here. In most cases, you can keep the defaults.

Local IP Address The default value is 192.168.1.1.

Subnet Mask The default value is 255.255.255.0.

Server Settings (DHCP)

The Router can be used as your network's DHCP (Dynamic Host Configuration Protocol) server, which automatically assigns an IP address to each PC on your network. Unless you already have one, it is highly recommended that you leave the Router enabled as a DHCP server.

DHCP Server DHCP is already enabled by factory default. If you already have a DHCP server on your network, or if you don't want a DHCP server, then select **Disabled** (no other DHCP features will be available). If you already have a DHCP server on your network, and you want this Router to act as a Relay for that DHCP Server, select **DHCP Relay**, then enter the DHCP Server IP Address. If you disable DHCP, assign a static IP address to the Router.

Starting IP Address Enter a value for the DHCP server to start with when issuing IP addresses. This value must be 192.168.1.2 or greater, but smaller than 192.168.1.254, because the default IP address for the Router is 192.168.1.1, and 192.168.1.255 is the broadcast IP address.

Maximum Number of DHCP Users Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. In order to determine the DHCP IP Address range, add the starting IP address (e.g., 100) to the number of DHCP users.

Client Lease Time This is the amount of time a DHCP client can keep the assigned IP address before it sends a renewal request to the DHCP server.

Static DNS 1-3 If applicable, enter the IP address(es) of your DNS server(s).

WINS The Windows Internet Naming Service (WINS) provides name resolution service (similar to DNS) in Windows networks. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.

Static IP Mapping

Static IP Mapping is used to bind a specific IP address to a specific MAC address. This helps external (WAN) users to access LAN servers that are advertised through NAPT port forwarding. You can define up to 50 entries.

Static IP Address Enter the IP address to be mapped.

MAC Address Enter the MAC address to be mapped.

Host Name Enter the host name to be mapped.

Click **Add** to create the entry and add it to the list. To modify an existing entry, select it from the list, edit the appropriate field(s), and then click **Modify**. To delete an entry, select it and click **Remove**.

IPv6

IPv6 Address If your network has implemented IPv6, enter the proper IPv6 address in this field.

Prefix Length Enter the appropriate IPv6 prefix length.

Router Advertisement Enabling this option allows IPv6 hosts to configure their IP addresses automatically using the IPv6 prefix broadcast by the router.

DHCPv6

To enable the DHCP v6 feature, select **Enable**. To disable DHCP v6, select **Disable**.

Lease time Enter the lease time in minutes.

DHCP6 address range start Enter the starting DHCP v6 IP address.

DHCP6 address range end Enter the ending DHCP v6 IP address.

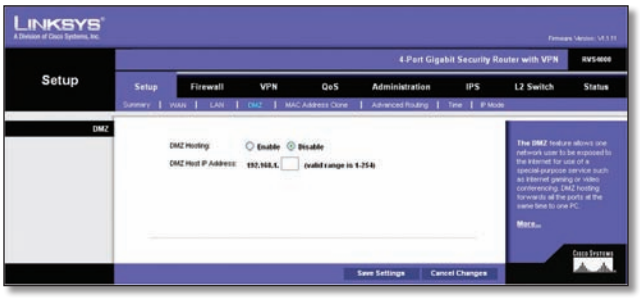
Primary DNS Enter the Primary DHCP v6 DNS server address.

Secondary DNS Enter the Secondary DHCP v6 DNS server address.

Click **Save Settings** to save your changes, or click **Cancel Changes** to undo your changes.

Setup > DMZ

The DMZ screen allows one local PC to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing. Whereas Port Range Forwarding can only forward a maximum of 10 ranges of ports, DMZ hosting forwards all the ports for one PC at the same time.



Setup > DMZ

DMZ Hosting This feature allows one local PC to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing. To use this feature, select **Enable**. To disable the DMZ feature, select **Disable**.

DMZ Host IP Address To expose one PC, enter the computer's IP address.

Click **Save Settings** to save your changes, or click **Cancel Changes** to undo your changes.

Setup > MAC Address Clone

Some ISPs require that you register a MAC address. This feature "clones" your network adapter's MAC address onto the Router, and prevents you from having to call your ISP to change the registered MAC address to the Router's MAC address. The Router's MAC address is a 12-digit code assigned to a unique piece of hardware for identification.

Setup > MAC Address Clone

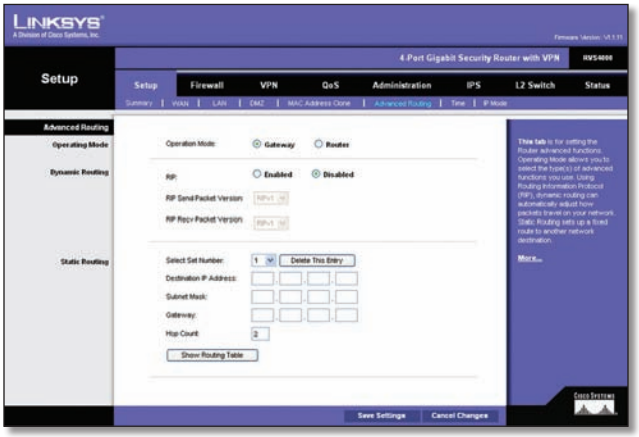
MAC Address Clone Select **Enabled** or **Disabled** from the drop-down menu.

MAC Address Enter the MAC Address registered with your ISP in this field.

Clone My PC's MAC When MAC Address Clone is enabled, click this button to copy the MAC address of the network adapter in the computer that you are using to connect to the Web interface.

Click **Save Settings** to save the MAC Cloning settings or click **Cancel Changes** to undo your changes.

Setup > Advanced Routing



Setup > Advanced Routing

Operating Mode

Operation Mode Select the Operating mode in which this Router will function.:

- **Gateway** This is the normal mode of operation. This allows all devices on your LAN to share the same WAN (Internet) IP address. In Gateway mode, the NAT (Network Address Translation) mechanism is enabled.
- **Router** You either need another Router to act as the Internet Gateway, or all PCs on your LAN must be assigned (fixed) Internet IP addresses. In Router mode, the NAT mechanism is disabled.

Dynamic Routing

The Router's dynamic routing feature can be used to automatically adjust to physical changes in the network's layout. The Router can use the dynamic RIP protocol to calculate the most efficient route for the network's data packets to travel between the source and the destination, based upon the shortest paths. The RIP protocol regularly broadcasts routing information to other routers on the network.

RIP (Routing Information Protocol) If you want the Router to use the RIP protocol, select **Enabled**; otherwise, keep the default setting, **Disabled**.

RIP Send Packet Version Choose the TX protocol you want for transmitting data on the network: **RIPv1** or **RIPv2**. This should match the version supported by other Routers on your LAN.

RIP Recv Packet Version Choose the RX protocol you want for receiving data from the network: **RIPv1** or **RIPv2**. This should match the version supported by other Routers on your LAN.

Static Routing

Sometimes you will prefer to use static routes to build your routing table instead of using dynamic routing protocols. Static routes do not require CPU resources to exchange routing information with a peer router. You can also use static routes to reach peer routers that do not support dynamic routing protocols. Static routes can be used together with dynamic routes. Be careful not to introduce routing loops in your network.

To set up static routing, you should add route entries in the routing table that tell the Router where to forward packets to specific IP destinations.

Enter the following data to create a static route entry:

Select Set Number Select the set number (routing table entry number) that you wish to view or configure. If necessary, click **Delete This Entry** to clear the entry.

Destination IP Address Enter the network address of the remote LAN segment. For a standard Class C IP domain, the network address is the first three fields of the Destination LAN IP, while the last field should be zero.

Subnet Mask Enter the Subnet Mask used on the destination LAN IP domain. For Class C IP domains, the Subnet Mask is **255.255.255.0**.

Gateway If this Router is used to connect your network to the Internet, then your gateway IP is the Router's IP Address. If you have another router handling your network's Internet connection, enter the IP Address of that router instead.

Hop Count This value gives the number of nodes that a data packet passes through before reaching its destination. A node is any device on the network, such as switches, PCs, etc. The maximum hop count value is 16.

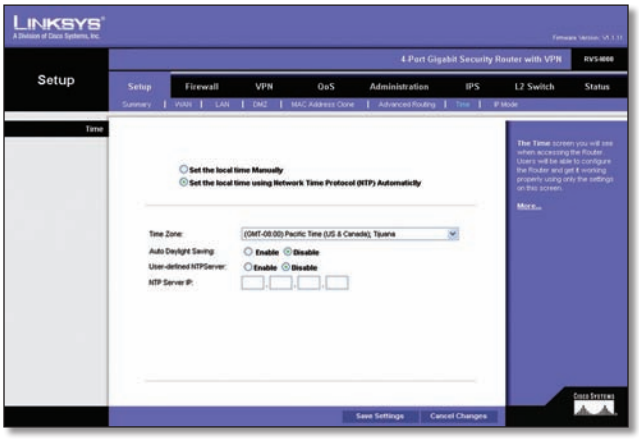
Show Routing Table Click this button to show the routing table established either through dynamic or static routing methods.

Inter-VLAN Routing

Inter-VLAN Routing Select **Enable** to allow packets to be routed between VLANs that are in different subnets. The default is **Enable**.

Click **Save Settings** to save the Routing settings or click **Cancel Changes** to undo your changes.

Setup > Time



Setup > Time

Set the local time Manually If you wish to enter the time and date manually, select this option, then select the Date from the drop-down fields and enter the hour, minutes, and seconds in the *Time* fields using 24-hour format. For example, for 10:00 pm, enter **22** in the hours field, **0** in the minutes field, and **0** in the seconds field.

Set the local time using Network Time Protocol (NTP) Automatically If you wish to use a Network Time Protocol server to set the time and date, select this option, then complete the following fields.

Time Zone Select the time zone for your location and your time setting is synchronized over the Internet.

Auto Daylight Saving If your location observes daylight savings time, select the **Enable** option.

User-defined NTP Server To specify a user-defined NTP server, select the Enable option, then enter the NTP Server's IP address in the *NTP Server IP* field.

NTP Server IP If the *User-defined NTP Server* option is set to **Enable**, enter the IP address of the NTP server.

Click **Save Settings** to save your settings or click **Cancel Changes** to undo your changes.

Setup > IP Mode

Setup > IP Mode

IPv4 Only Select this option to use IPv4 on the Internet and local network.

Dual-Stack IP Select this option to use IPv4 on the Internet and IPv4 and IPv6 on the local network. Then select how the IPv6 hosts will connect to the Internet:

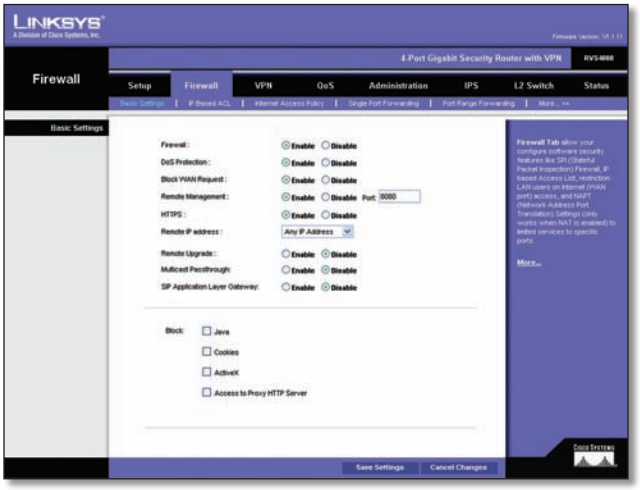
- **NAPT-PT** This allows an IPv6-only host on your LAN to connect to IPv4-only hosts on the WAN using address-translation and protocol-translation (per RFC2766).
- **6to4 Tunnel** This allows your IPv6 network to connect to other IPv6 networks via tunnels through IPv4 (per RFC3056). The remote router also needs to support 6to4.

Click **Save Settings** to save your settings or click **Cancel Changes** to undo your changes.

Firewall

From the Firewall Tab, you can configure the Router to deny or allow specific internal users from accessing the Internet. You can also configure the Router to deny or allow specific Internet users from accessing the internal servers. You can set up different packet filters for different users that are located on internal (LAN) side or external (WAN) side based on their IP addresses or their network Port number.

Firewall > Basic Settings



Firewall > Basic Settings

Firewall When this feature is enabled, the Router's NAT firewall feature is enabled.

DoS Protection When this feature is enabled, the Router will block DoS (Denial of Service) attacks. A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you can not use it.

Block WAN Request When this feature is enabled, the Router filters out anonymous requests from the WAN.

Remote Management This feature allows you to use an http or https port to remotely manage the Router. To enable this feature, select **Enable** and enter the port number in the *Port* field, then configure the *HTTPS* and *Remote IP address* settings that appear below.

HTTPS This option limits access to the Web-based Utility from the WAN to https sessions only. An https session uses SSL encryption, providing better protection for your remote session than http. The default is **Enable**.

- **Remote IP address** Select the appropriate value to specify which external IP address(es) can access the Router:
- **Any IP Address** Allows access from any external IP address.
- **Single IP Address** Allows access from the single IP address that you enter in the field provided.
- **IP Range** Allows access from a range of IP addresses that you enter in the field provided.
- **Subnet** Allows access from the Subnet that you enter in the field provided.

Remote Upgrade This option allows you to upgrade the Router remotely. To allow remote upgrade, select Enable. The Remote Management feature must be set to Enable as well. The default is **Disable**.

Multicast Passthrough If an IGMP Proxy running on the Router, set this to Enable to cause the Router to allow IP Multicast traffic to come in from the Internet. The default is **Disable**.

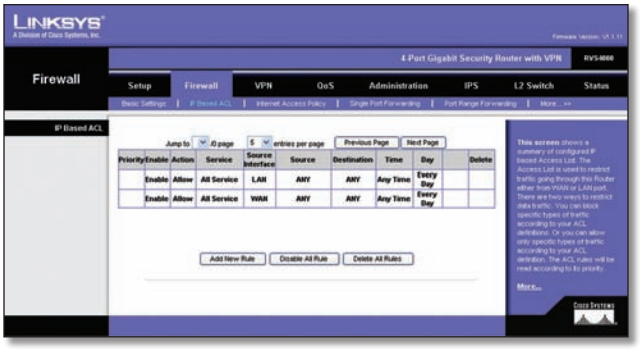
SIP Application Layer Gateway When this feature is enabled, the SIP Application Layer Gateway (ALG) allows Session Initiation Protocol (SIP) packets (used for Voice over IP) to traverse the NAT firewall. This feature can be disabled if the VoIP service provider is using other NAT traversal solutions such as STUN, TURN, and ICE.

Block Place a checkmark next to the Web features that you wish to restrict.

- **Java** Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language.
- **Cookies** A cookie is data stored on your PC and used by Internet sites when you interact with them, so you may not want to deny cookies.
- **ActiveX** ActiveX is a Microsoft (Internet Explorer) programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites using this programming language. Also, Windows Update uses ActiveX, so if this is blocked, Windows update will not work.
- **Access to Proxy HTTP Server** If local users have access to WAN proxy servers, they may be able to circumvent the Router's content filters and access Internet sites blocked by the Router. Denying Proxy will block access to any WAN proxy servers.

Firewall > IP Based ACL

The IP-Based ACL screen allows you to create an Access Control List (ACL) with up to 50 rules. Each ACL rule denies or allows access to the network based on various criteria including priority, service type, interface, source IP address, destination IP address, day of the week, and time of day.



Firewall > IP Based ACL

Priority This is the rule's priority.

Enable This indicates whether the rule is enabled or disabled.

Action. This is the rule's action, either Allow or Deny.

Service This is the service(s) to which the rule applies.

Source Interface This is the source interface, either WAN, LAN, or ANY.

Source This is the source IP address, which can be one specific IP address, ANY (all IP addresses), a range of IP addresses, or a specific IP subnet.

Destination This is the destination IP address, which can be one specific IP address, ANY (all IP addresses), a range of IP addresses, or a specific IP subnet.

Time The time of day when the rule is in effect, either Any Time (24 hours) or a specific start and end time.

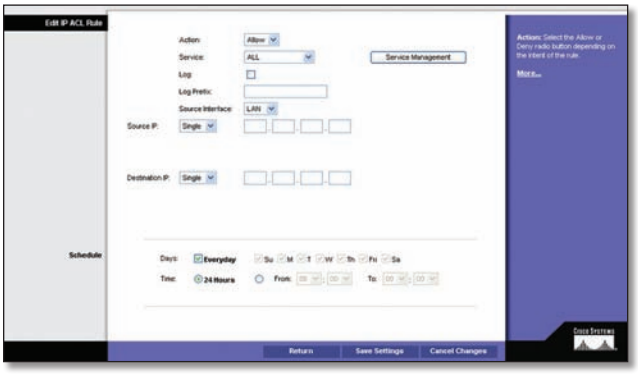
Day The day(s) of the week when the rule is in effect. This may be Any Day or a user-specified set of days.

Edit button Click Edit at the end of a row to edit the associated rule.

Delete button Click Delete at the end of a row to delete the associated rule.

To add a new rule to the ACL rule table, click **Add New Rule** and the *Edit IP ACL Rule* screen appears. Follow the instructions in the section below to create a new ACL rule. To disable all the rules without deleting them, click **Disable All Rules**. To delete all the rules from the table, click **Delete All Rules**.

Editing IP ACL Rules



Edit IP ACL Rule

Action Select the desired action, **Allow** or **Deny**, from the drop-down menu.

Service Select the service types to which the rule will apply. You can either select one of the predefined services in the drop-down menu; select **ALL** to allow or deny all types of IP traffic; or define a new service by clicking **Service Management** to bring up the *Service Management* screen, then the new service's Name, select the Type (TCP, UDP, or TCP/UDP), enter the Start Port and Finish Port, then click **Save**. The new service will then appear in the drop-down menu on the *Edit IP ACL Rule* screen.

Log Select this option to log all traffic that is filtered by this rule.

Log Prefix Enter a text string that will be prepended to each matched event in the log.

Source Interface Select the source interface, **WAN**, **LAN**, or **ANY**, from the drop-down menu.

Source IP To apply the rule to one source IP address, select **Single** from the drop-down menu, then enter the address in the field. To apply the rule to all source IP addresses, select **ANY** from the drop-down menu. To apply the rule to a range of IP addresses, select **Range** and enter the starting and ending IP addresses. To apply the rule to a subnet, select **Net** and enter the IP address and subnet mask.

Destination IP To apply the rule to one destination IP address, select **Single** from the drop-down menu, then enter the address in the field. To apply the rule to all destination IP addresses, select **ANY** from the drop-down menu. To apply the rule to a range of IP addresses, select **Range** and enter the starting and ending IP addresses. To apply the rule to a subnet, select **Net** and enter the IP address and subnet mask.

Days To make the rule apply on a daily basis, select **Everyday**. To make the rule apply on specific days of the week only, select the desired days.

Time To make the rule apply for an entire day, select **24 Hours**. To make the rule apply only during a specific period of the day, enter the starting time in the *From* field and the ending time in the *To* field.

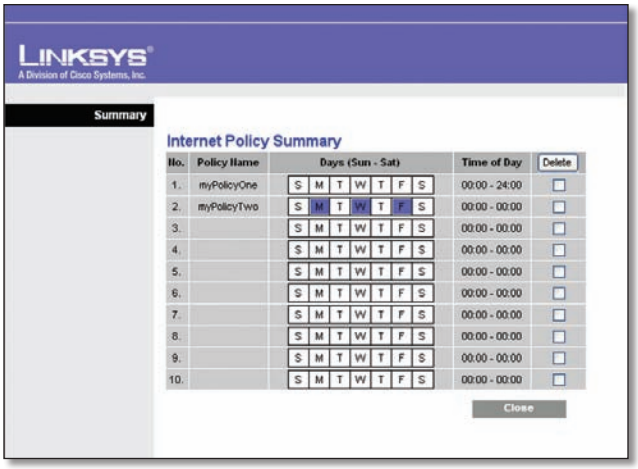
Click **Save Settings** to save your settings. Click **Cancel Changes** to cancel your changes. Click **Return** to return to the IP-Based ACL screen.

Firewall > Internet Access Policy

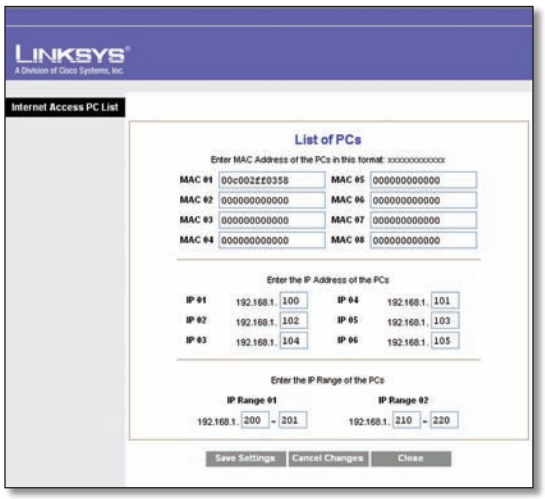
Firewall > Internet Access Policy

Access can be managed by a policy. Use the settings on this screen to establish an access policy. Selecting a policy from the drop-down menu will display that policy's settings. You can then perform the following operations:

- Create a Policy—see instructions below.
- Delete the current policy—click **Delete**.
- View all policies—click **Summary** to display the *Internet Policy Summary* popup which lists all of the Internet access policies and includes the following information: No., Policy Name, Days, Time, and a checkbox to delete (clear) the policy. To delete a policy, check the checkbox in the *Delete* column, and click **Delete**.
- View or change the PCs covered by the current policy—click **Edit List of PCs** to display the *List of PCs* popup.



Internet Policy Summary



List of PCs

On the *List of PCs* popup, you can define PCs by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs.

To create an Internet Access policy:

1. Select the desired policy number from the *Internet Access Policy* drop-down menu.
2. Enter a Policy Name in the field provided.
3. To enable this policy, set the *Status* option to **Enable**.
4. Click **Edit List of PCs** to select which PCs will be affected by the policy. The *List of PCs* popup will appear. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click **Save Settings** to apply your changes.
5. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* popup.
6. Decide which Days and what Times you want this

policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.

7. If you wish to block access to Web sites, use the **Website Blocking by URL Address** or **Website Blocking by Keyword** feature.
   - **Website Blocking by URL Address**. Enter the URL or Domain Name of the web sites you wish to block.
   - **Website Blocking by Keyword**. Enter the keywords you wish to block in the fields provided. If any of these Keywords appears in the URL of a web site, access to the site will be blocked. Note that only the URL is checked, not the content of each Web page.

Click **Save Settings** to save the policy settings you have entered. Click **Cancel Changes** to cancel any changes you have entered.

Firewall > Single Port Forwarding

Firewall > Single Port Forwarding

Application Enter the name of the application you wish to configure.

External Port This is the port number used by the server or Internet application. Internet users must connect using this port number. Check with the software documentation of the Internet application for more information.

Internal Port This is the port number used by the Router when forwarding Internet traffic to the PC or server on your LAN. Normally, this is the same as the External Port number. If it is different, the Router performs a "Port Translation", so that the port number used by Internet users is different from the port number used by the server or Internet application.

For example, you could configure your Web Server to accept connections on both port 80 (standard) and port 8080. Then enable Port Forwarding, and set the External Port to 80, and the Internal Port to 8080. Now, any traffic from the Internet to your Web server will be using port 8080, even though the Internet users used the standard port, 80. (Users on the local LAN can and should connect to your Web Server using the standard port 80.)

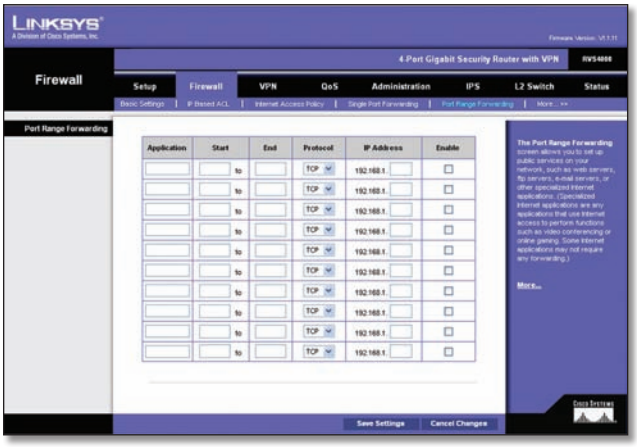
Protocol Select the protocol used for this application, TCP and/or UDP.

IP Address For each application, enter the IP address of the PC running the specific application.

Enabled Click the **Enabled** checkbox to enable port forwarding for the relevant application.

Click **Save Settings** to save the settings you have entered. Click **Cancel Changes** to cancel any changes you have entered.

Firewall > Port Range Forwarding



Firewall > Port Range Forwarding

Application Enter the name of the application you wish to configure.

Start This is the beginning of the port range. Enter the beginning of the range of port numbers (external ports) used by the server or Internet application. Check with the software documentation of the Internet application for more information if necessary.

End This is the end of the port range. Enter the end of the range of port numbers (external ports) used by the server or Internet application. Check with the software documentation of the Internet application for more information if necessary.

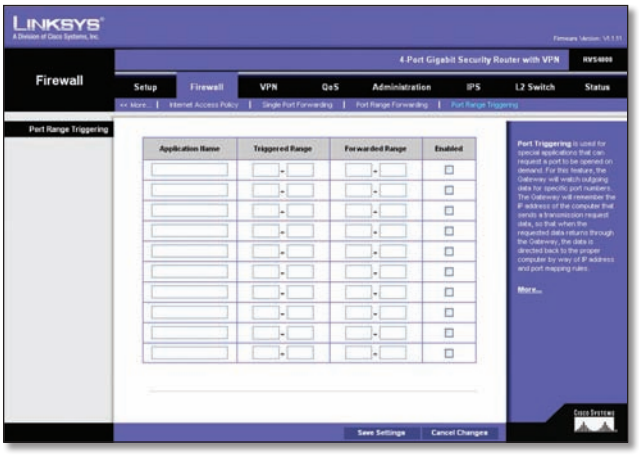
Protocol Select the protocol(s) used for this application, TCP and/or UDP.

IP Address For each application, enter the IP address of the PC running the specific application.

Enabled Click the **Enabled** checkbox to enable port range forwarding for the relevant application.

Click **Save Settings** to save the settings you have entered. Click **Cancel Changes** to cancel any changes you have entered.

Firewall > Port Range Triggering



Firewall > Port Range Triggering

Application Name Enter the name of the application you wish to configure.

Triggered Range For each application, list the triggered port number range. These are the ports used by outgoing traffic. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the Triggered Range. In the second field, enter the ending port number of the Triggered Range.

Forwarded Range For each application, list the forwarded port number range. These are the ports used by incoming traffic. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the Forwarded Range. In the second field, enter the ending port number of the Forwarded Range.

Enabled Click the **Enabled** checkbox to enable port range triggering for the relevant application.

Click **Save Settings** to save the settings you have entered. Click **Cancel Changes** to cancel any changes you have entered.

VPN

VPN > Summary

VPN > Summary

Tunnels Used Displays the number of tunnels used.

Tunnel(s) Available Displays the number of available tunnels.

Detail button Click **Detail** to display more tunnel information.

Tunnel Status

No. Displays the number of the tunnel.

Name Displays the name of the tunnel, as defined by the Tunnel Name field on the *VPN* > *IPSec VPN* screen.

Status Displays the tunnel's status: Connected, Hostname Resolution Failed, Resolving Hostname, or Waiting for Connection.

Phase2 Enc/Auth. Displays the Phase 2 Encryption type (3DES), Authentication type (MD5 or SHA1), and Group (768-bit, 1024-bit, or 1536-bit) that you chose in the *VPN* > *IPSec VPN* screen.

Local Group Displays the IP address and subnet of the local group.

Remote Group Displays the IP address and subnet of the remote group.

Remote Gateway Displays the IP address of the remote gateway.

Tunnel Test Click **Connect** to verify the tunnel status; the test result is updated in the *Status* column. If the tunnel is connected, you can disconnect the IPSec VPN connection by clicking **Disconnect**.

Config Click **Edit** to change the tunnel's settings. Click **Trash** to delete all of the tunnel's settings.

Tunnel(s) Enabled Displays the total number of currently enabled tunnels.

Tunnel(s) Defined Displays the number of tunnels currently defined. This number will be greater than the *Tunnels Enabled* field if any defined tunnels have been disabled.

VPN Clients Status

No. Displays the user number from 1 to 5.

Username. Displays the username of the VPN Client.

Status Displays the connection status of the VPN Client.

Start Time Displays the start time of the most recent VPN session for the specified VPN Client.

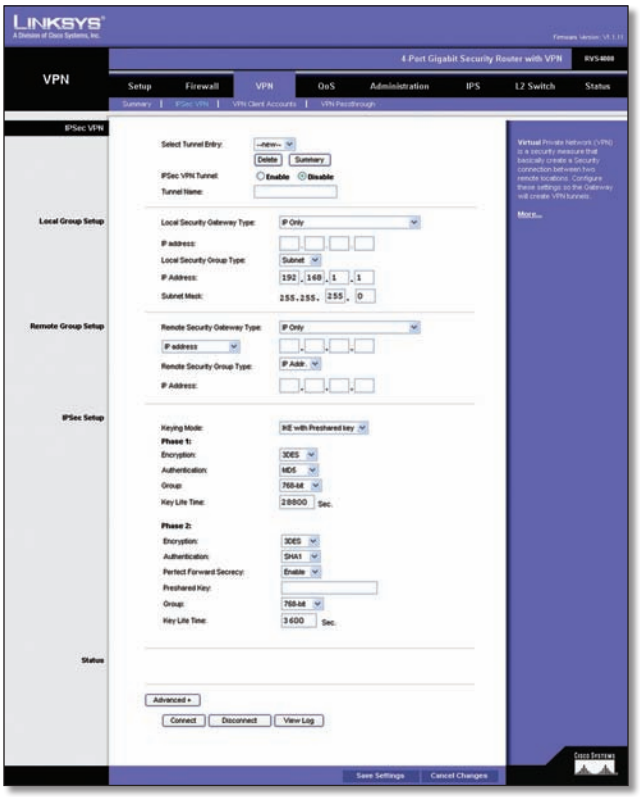
End Time Displays the end time of a VPN session if the VPN Client has disconnected.

Duration Displays the total connection time of the latest VPN session.

Disconnect Check the *Disconnect* checkbox at the end of each row in the VPN Clients Table and click the **Disconnect** button to disconnect a VPN Client session.

VPN > IPSec VPN

The *VPN > IPSec VPN* screen is used to create and configure a Virtual Private Network (VPN) tunnel.



VPN > IPSec VPN

Select Tunnel Entry To create a new tunnel, select **new.** To configure an existing tunnel, select it from the drop-down menu.

Delete Click this button to delete all settings for the selected tunnel.

Summary Clicking this button shows the settings and status of all enabled tunnels.

IPSec VPN Tunnel Check the **Enable** option to enable this tunnel.

Tunnel Name Enter a name for this tunnel, such as "Anaheim Office".

Local Group Setup

Local Security Gateway Type This has two settings, **IP Only** and **IP + Domain Name (FQDN) Authentication**.

- **IP Only** If this is selected, the RVS4000's WAN IP address automatically appears in the *IP Address* field.
- **IP + Domain Name (FQDN) Authentication** This is the same as **IP Only**, but includes a domain name for greater security. Enter an arbitrary domain name in the *Domain Name* field. The Router's WAN IP address automatically appears in the *IP Address* field.

Local Security Group Type Select the local LAN user(s) behind the router that can use this VPN tunnel. This may be a single IP address or Sub-network. Notice that the Local Security Group Type must match the other router's Remote Security Group Type.

IP Address Enter the IP address on the local network.

Subnet Mask If the Local Security Group Type is set to **Subnet**, enter the mask to determine the IP addresses on the local network.

Remote Group Setup

Remote Security Gateway Type Select either **IP Only** or **IP + Domain Name (FQDN) Authentication**. The setting should match the Local Security Gateway Type for the VPN device at the other end of the tunnel.

- **IP Only** Select this to specify the remote device that will have access to the tunnel. Then either select **IP Address** from the drop-down menu and enter the remote gateway's WAN IP address in the *IP Address* field, or select **IP by DNS Resolved** from the drop-down menu and enter the remote gateway's domain name in the *Domain Name* field.
- **IP + Domain Name (FQDN) Authentication** This is the same as **IP Only** but includes a domain name for greater security. Enter an arbitrary domain name in the *Domain Name* field. Then select either **IP Address** or **IP by DNS Resolved** from the drop-down menu, and fill in the *IP Address* field or *Domain Name* field.

Remote Security Group Type Select the remote LAN user(s) behind the remote gateway who can use this VPN tunnel. This may be a single IP address or a Sub-network. Note that the Remote Security Group Type must match the other router's Local Security Group Type.

IP Address Enter the IP address on the remote network.

Subnet Mask If the Remote Security Group Type is set to **Subnet**, enter the mask to determine the IP addresses on the remote network.

IPSec Setup

Keying Mode The router supports both automatic and manual key management. When choosing automatic key management, IKE (Internet Key Exchange) protocols are used to negotiate key material for SA (Security Association). If manual key management is selected, no key negotiation is needed. Basically, manual key management is used in small static environments or for troubleshooting purposes. Note that both sides must use the same Key Management method.

Phase 1

- **Encryption** The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. Only 3DES is supported. Notice that both sides must use the same Encryption method.
- **Authentication** Authentication determines a method to authenticate the ESP packets. Either MD5 or SHA1 may be selected. Notice that both sides (VPN endpoints) must use the same Authentication method.
  - **MD5** A one-way hashing algorithm that produces a 128-bit digest.
  - **SHA1** A one-way hashing algorithm that produces a 160-bit digest.
- **Group** The Diffie-Hellman (DH) group to be used for key exchange. Select the 768-bit (Group 1), 1024-bit (Group 2), or 1536-bit (Group 5) algorithm. Group 5 provides the most security, Group 1 the least.
- **Key Life Time** This specifies the lifetime of the IKE-generated key. If the time expires, a new key will be renegotiated automatically. Enter a value from 300 to 100,000,000 seconds. The default is **28800** seconds.

Phase 2

- **Encryption** The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. Only 3DES is supported. Note that both sides must use the same Encryption method.
- **Authentication** Authentication determines a method to authenticate the ESP packets. Either MD5 or SHA1 may be selected. Note that both sides (VPN endpoints) must use the same Authentication method.
  - **MD5** A one-way hashing algorithm that produces a 128-bit digest.
  - **SHA1** A one-way hashing algorithm that produces a 160-bit digest.
- **Perfect Forward Secrecy** If PFS is enabled, IKE Phase 2 negotiation will generate a new key material for IP traffic encryption and authentication. Note that both sides must have this selected.
- **Preshared Key** IKE uses the Preshared Key field to authenticate the remote IKE peer. Both character and hexadecimal values are acceptable in this field; e.g., "My_@123" or "0x4d795f40313233". Note that both sides must use the same Preshared Key.
- **Group** The Diffie-Hellman (DH) group to be used for key exchange. Select the 768-bit (Group 1), 1024-bit (Group 2), or 1536-bit (Group 5) algorithm. Group 5 provides the most security, Group 1 the least.
- **Key Life Time** This specifies the lifetime of the IKE-generated key. If the time expires, a new key will be renegotiated automatically. Enter a value from 300 to 100,000,000 seconds. The default is **3600** seconds.

Status

Status Displays the connection status for the selected tunnel. The state is either connected or disconnected.

Connect Click this button to establish a connection for the current VPN tunnel. If you have made any changes, click Save Settings first to apply your changes.

Disconnect Click this button to break a connection for the current VPN tunnel.

View Log Click this button to view the VPN log, which shows details of each tunnel established.

Advanced Click this button to display the following additional settings.

- **Aggressive Mode** This is used to specify the type of Phase 1 exchange, Main mode or Aggressive mode. Check the box to select Aggressive Mode or leave the box unchecked (default) to select Main mode. Aggressive mode requires half of the main mode messages to be exchanged in Phase 1 of the SA exchange. If network security is preferred, select Main mode.
- **NetBios Broadcasts** Check the box to enable NetBIOS traffic to pass through the VPN tunnel. By default, the RVS4000 blocks these broadcasts.

Click **Save Settings** to save the settings you have entered. Click **Cancel Changes** to cancel any changes you have entered.

VPN > VPN Client Accounts

Use this page to administer your VPN Client users. Enter the information at the top of the screen and the users you've entered will appear in the list at the bottom, showing their status. This will work with the Linksys QuickVPN client only. (The Router supports up to five Linksys QuickVPN Clients by default. Additional QuickVPN Client licenses can be purchased separately. See www.linksys.com for more information.)

VPN > VPN Client Accounts

Username Enter the username using any combination of keyboard characters.

Password Enter the password you would like to assign to this user.

Re-enter to Confirm Retype the password to ensure it has been entered correctly.

Allow User to Change Password This option determines whether the user is allowed to change their password.

VPN Client List Table

No. Displays the user number.

Active When checked, the designated user can connect, otherwise the VPN client account is disabled.

Username Displays the username.

Edit This button is used to modify the username or password, and to allow/deny the user permission to change their password.

Remove This button is used to delete a user account.

Certificate Management

This section allows you to manage the certificate used for securing the communication between the router and QuickVPN clients.

Generate Click this button to generate a new certificate to replace the existing certificate on the router.

Export for Admin Click this button to export the certificate for administrator. A dialog will ask you to specify where you want to store your certificate. The default file name is "RVS4000_Admin.pem" but you can use another name. The certificate for administrator contains the private key and needs to be stored in a safe place as a backup. If the router's configuration is reset to the factory default, this certificate can be imported and restored on the router.

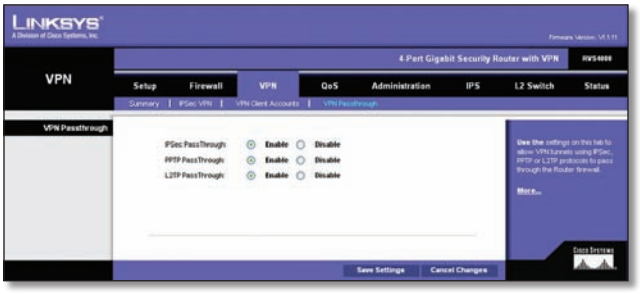
Export for Client Click this button to export the certificate for client. A dialog will ask you where you want to store your certificate. The default file name is "RVS4000_Client.pem" but you can use another name. For QuickVPN users to securely connect to the router, this certificate needs to be placed in the install directory of the QuickVPN client.

Import Click this button to import a certificate previously saved to a file using **Export for Admin** or **Export for Client**. Enter the file name in the field or click **Browse** to locate the file on your computer, then click **Import**.

Certificate Last Generated or Imported This displays the date and time when a certificate was last generated or imported.

Click **Save Settings** to save your settings. Click **Cancel Changes** to cancel any changes you have entered.

VPN > VPN Passthrough



VPN > VPN Passthrough

IPSec PassThrough Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPSec Passthrough is enabled by default to allow IPSec tunnels to pass through the Router. To disable IPSec Passthrough, select **Disabled**.

PPTP PassThrough Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP Passthrough is enabled by default. To disable it, select **Disabled**.

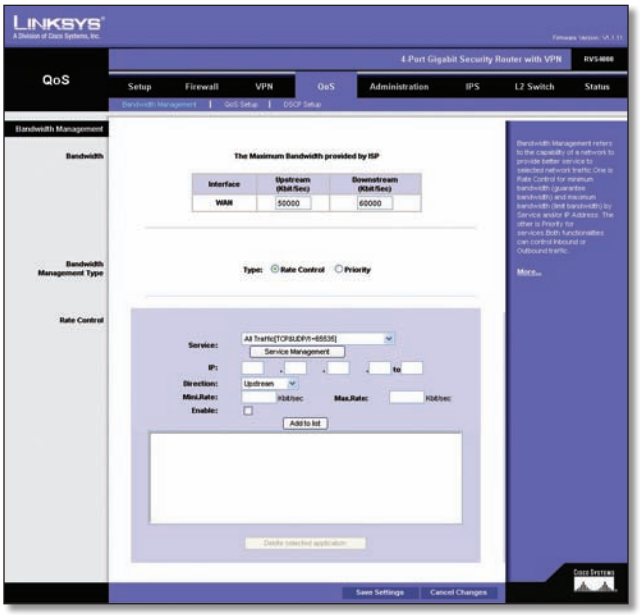
L2TP PassThrough Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. L2TP Passthrough is enabled by default. To disable L2TP Passthrough, select **Disabled**.

Click **Save Settings** to save your settings. Click **Cancel Changes** to cancel any changes you have entered.

QoS

QoS (Quality of Service) allows you to perform Bandwidth Management, by either **Rate Control** or **Priority**. You can also configure QoS Trust Mode and the DSCP settings.

QoS > Bandwidth Management



QoS > Bandwidth Management - Rate Control

Bandwidth

This section lets you specify the maximum bandwidth provided by the ISP on the WAN interface, for both the upstream and downstream directions.

Bandwidth Management Type

Type The desired type of bandwidth management, either **Rate Control** (default) or **Priority**. Depending on your selection, the lower portion of the screen displays either the Rate Control section or the Priority section.

Rate Control

Service Select the service from the drop-down menu. If it does not contain the service you need, click **Service Management** to add the service.

IP Enter the IP address or IP range you need to control. The default is zero which includes all internal IP addresses.

Direction Select **Upstream** for outbound traffic or **Downstream** for inbound traffic.

Mini. Rate Enter the minimum rate for the guaranteed bandwidth.

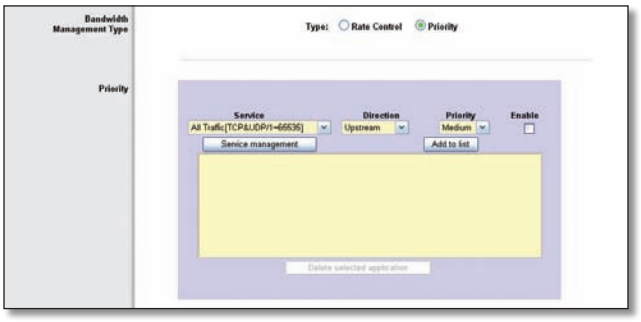
Max. Rate Enter the maximum rate for the guaranteed bandwidth.

Enable Check this box to enable this Rate Control Rule.

Add to list After a rule is set up, click this button to add it to the list. The list can contain a maximum of 15 entries.

Delete selected application Click this button to delete a rule from the list.

Priority



QoS > Bandwidth Management - Priority

Service Select the service from the drop-down menu. If it does not contain the service you need, click **Service Management** to add the service.

Direction Select **Upstream** for outbound traffic or **Downstream** for inbound traffic from the drop-down menu.

Priority Select **High**, **Medium**, **Normal**, or **Low** priority for the service. The default is **Medium**.

Enable Check this box to enable this Priority Rule.

Add to list After a rule is set up, click this button to add it to the list. The list can contain a maximum of 15 entries.

Delete selected application Click this button to delete a rule from the list.

Click **Save Settings** to save your settings. Click **Cancel Changes** to cancel any changes you have entered.

QoS > QoS Setup

The *QoS Setup* screen allows users to configure QoS Trust Mode for each LAN port.

QoS > QoS Setup

Port ID The number of the LAN port.

Trust Mode Select either **Port**, **CoS**, or **DSCP.** The default is **Port**.

Default CoS/Port Priority If Trust Mode is set to **Port**, select the port priority from **1** to **4** from the drop-down menu. If Trust Mode is set to **CoS**, select the default CoS priority from **0** to **7** from the drop-down menu.

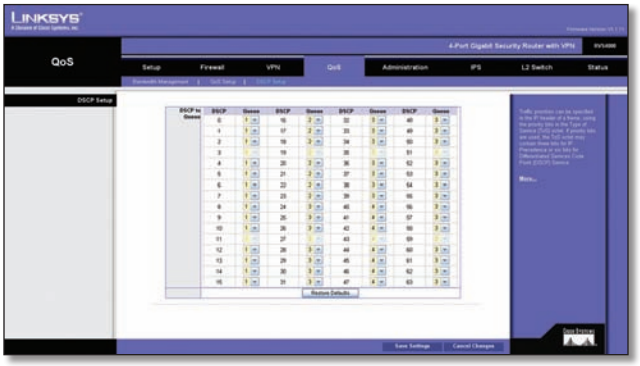
CoS Setup

Priority The CoS priority from **0** to **7**.

Queue Select the traffic forwarding queue, **1** to **4**, to which the CoS priority is mapped.

Click **Save Settings** to save your settings. Click **Cancel Changes** to cancel any changes you have entered.

QoS > DSCP Setup



QoS > DSCP Setup

DSCP The Differentiated Services Code Point value in the incoming packet.

Queue Select the traffic forwarding queue, **1** to **4**, to which the DSCP priority is mapped.

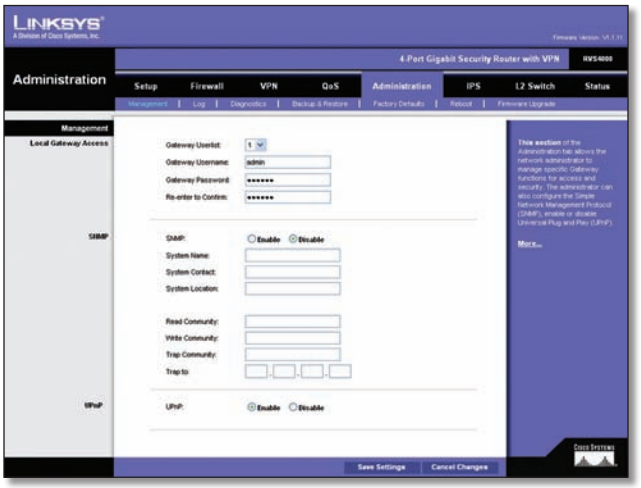
Restore Defaults Click this button to restore the default DSCP values.

Click **Save Settings** to save your settings. Click **Cancel Changes** to cancel any changes you have entered.

Administration

The Administration tab provides access to system administration settings and tools. It includes the following screens:

Administration > Management



Administration > Management

Local Gateway Access

Gateway Userlist Select the desired Gateway User List.

Gateway Username Enter the user name here.

Gateway Password Enter the password.

Re-enter to Confirm Retype the password in this field.

SNMP

SNMP Select Enable if you wish to use SNMP. To use SNMP, you need SNMP software on your PC.

System Name Enter a suitable name. This name will be used to identify this device, and will be displayed by your SNMP software.

System Contact Enter contact information for the system.

System Location Enter the location of the system.

Read Community Enter the SNMP community name for SNMP "Get" commands.

Write Community Enter the SNMP community name for SNMP "Set" commands.

Trap Community Enter the SNMP community name for SNMP "Trap" commands.

Trap To Enter the IP Address of the SNMP Manager to which traps will be sent. If desired, this may be left blank.

UPnP

Universal Plug and Play (UPnP) can used to set up public services on your network. When the UPnP function is enabled, Windows XP can add or delete entries to the underlined UPnP Forwarding Table. Some Internet games require enabling UPnP.

UPnP If you want to use UPnP, keep the default setting, **Enable**. Otherwise, select **Disable**.

Administration > Log

Administration > Log

Log Setting

Log Level Select the log level(s) that the Router should record. Log levels and their meanings are:

Log Levels

Level	Severity Name	Description
7	LOG_DEBUG	Debug-level message
6	LOG_INFO	Informational messages only
5	LOG_NOTICE	Normal but significant condition
4	LOG_WARNING	Warning conditions
3	LOG_ERR	Error conditions
2	LOG_CRIT	Critical conditions
1	LOG_ALERT	Immediate action needed
0	LOG_EMERG	System unusable

Outgoing Log Select **Enable** to cause all outgoing packets to be logged. You can then click **View Outgoing Table** to display information on the outgoing packets including Source IP, Destination IP, and Service/Port number.

Incoming Log Select **Enable** to cause all incoming packets to be logged. You can then click **View Incoming Table** to display information on incoming packets including Source IP, Destination IP, and Service/Port number.

Email Alerts

Email Alerts Select **Enable** to cause an e-mail to be sent immediately if a DoS (Denial of Service) attack is detected. If enabled, fill in the e-mail address information in the remaining fields in this section.

Denial of Service Thresholds Enter the number of DoS (Denial of Service) attacks which need to be blocked by the built-in Firewall before an e-mail alert is sent. The minimum value is 20, the maximum value is 100.

Log Queue Length The default is **50** entries (Router will e-mail the log if there are more than 50 entries).

Log Time Threshold The default is **10** minutes (Router will e-mail the log every 10 minutes).

SMTP Mail Server Enter the address (domain name) or IP address of the SMTP (Simple Mail Transport Protocol) Server you use for outgoing e-mail.

Email Address for Alert Logs Enter the e-mail address the Log is to be sent to.

Return Email Address The e-mail will show this address as the Sender's address.

Enable SMTP Authentication If your SMTP server requires Authentication, you can enable it here, and enter the Username and Password.

E-mail Log Now Press this button to cause the log to be e-mailed immediately.

Syslog

Enable Syslog Select the checkbox if you want to use this feature.

Syslog Server Enter the IP Address in this field when **Enable Syslog** is checked.

Local Log

Local Log Enable this if you want to see a log of all incoming and outgoing URLs or IP addresses.

View Log Click this button when you wish to view the logs. A new window will appear with the log data.

Administration > Diagnostics

Administration > Diagnostics

Ping Test Parameters

Ping Target IP Enter the IP address or URL that you want to ping.

Ping Size Enter the size of the packet you want to use.

Number of Pings Enter the number of times you wish to ping the target device.

Ping Interval Enter the time period (milliseconds) between each ping.

Ping Timeout Enter the desired time period (milliseconds). If a response is not received within the defined ping period, the ping is considered to have failed.

Start Test Click this button to begin the test. A new screen will appear and display the test results.

Ping Result Displays the Ping status.

Traceroute Test Parameters

Traceroute Target Enter the target IP address for the traceroute test.

Start Test Click this button to begin the test. A new screen will appear and display the test results.

Cable Diagnostics

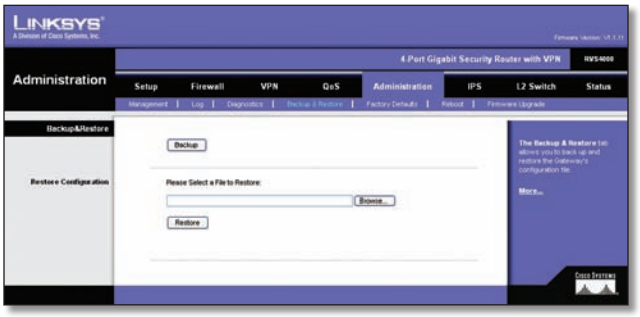
Port Select the port number from the drop-down menu.

Pair Identifies a specific pair (A, B, C, or D) in the cable. Each cable consists of 8 pins (4 pairs).

Cable Length Displays the length of the cable in meters.

Status Displays the status of the pair.

Administration > Backup & Restore



Administration > Backup & Restore

To download a copy of the current configuration and store the file on your PC, click **Backup** to start the download.

Restore Configuration

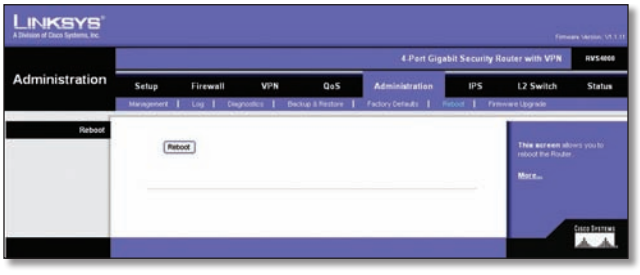
To restore a previously saved config file back to the Router, enter the file name in the field or click **Browse** to select the config file, then click **Restore** to upload the config file.

Administration > Factory Default

Administration > Factory Default

Restore Factory Defaults Click this button to reset all configuration settings to their factory default values. Any settings that have been saved will be lost when the default settings are restored. After clicking the button, another screen will appear. Click **OK** to continue. Another screen will appear while the system reboots.

Administration > Reboot



Administration > Reboot

Reboot Click this button to reboot the Router. This operation will not cause the Router to lose any of its stored settings.

Administration > Firmware Upgrade

Administration > Firmware Upgrade

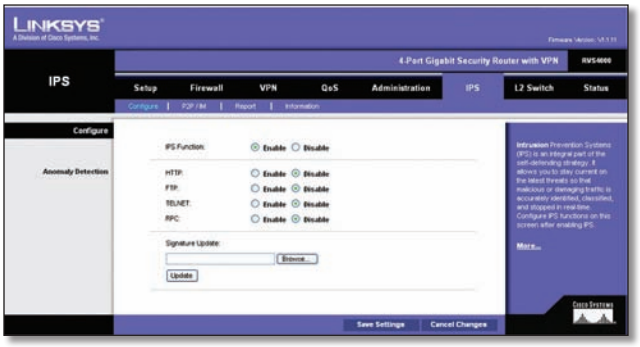
To upgrade firmware, download the latest firmware for the product from www.linksys.com, extract it to your computer, and perform the steps below:

File Type in the name of the extracted firmware upgrade file or click **Browse** to locate the file.

Start to Upgrade Once you have selected the appropriate file, click **Start to Upgrade** and follow the on-screen instructions to upgrade your firmware.

IPS

IPS > Configuration



IPS > Configuration

IPS Function Select **Enable** to enable or **Disable** to disable the IPS Function.

Anomaly Detection

HTTP Web attack signature is matched. HTTP request decoder will decode UTF-8 (1, 2, and 3 byte) code and normalize URI (according to those evasion methods mentioned in whisker) before pattern match.

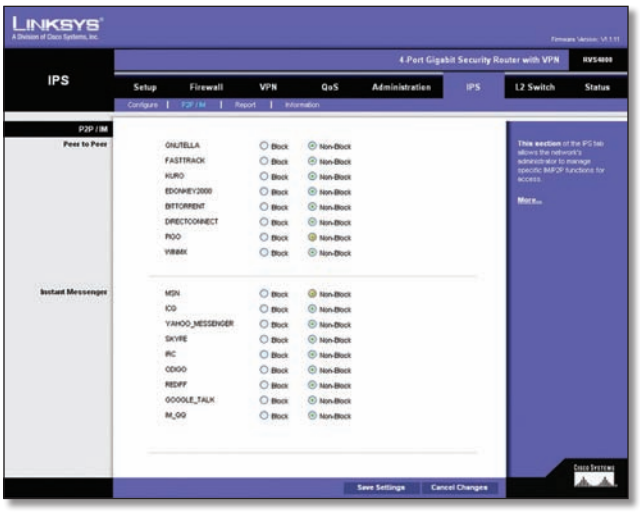
FTP FTP Bounce Detection and Inserting telnet opcodes into FTP command stream Detection.

TELNET Normalization of Telnet negotiation strings.

RPC RPC record fragging detection.

Signature Update Before upgrading the firmware, download and extract the Router firmware upgrade file from the Linksys website, www.linksys.com. Enter the firmware upgrade file name in the *Signature Update* field, or click **Browse** to find the file. Then click **Update** and follow the on-screen instructions.

IPS > P2P/IM



IPS > P2P/IM

Peer to Peer

Peer-to-peer file sharing applications can be blocked (**Block**) or allowed (**Non-Block**). The preconfigured file sharing networks are GNUTELLA (EZPEER), FASTTRACK, KURO, EDONKEY2000, BITTORRENT, DIRECTCONNECT, PIGO, and WINMX.

Instant Messenger

Instant messaging applications can be blocked (**Block**) or allowed (**Non-Block**). The preconfigured instant messaging applications are MSN, ICQ, YAHOO_MESSENGER, SKYPE, IRC, ODIGO, REDIFF, GOOGLE_TALK, and IM_QQ.

IPS > Report

Provides a graphical representation of the level of network traffic and attacks during the last twenty four hours.

Attacker

Displays the IP Address of attackers and the frequency (number of times) of the attacks.

Attack Category

Displays the category (type) of attack and the frequency (number of times) of the attacks.

IPS > Report

IPS > Information

IPS > Information

Signature Version Displays the version of the signature patterns in the Router that protects against malicious threats.

Last Time Upload This displays when the signature patterns in the router were last updated.

Protect Scope Lists the types of attacks that the Router's IPS feature protects against.

L2 Switch

L2 > Create VLAN

VLANs are logical subgroups of a Local Area Network (LAN) created via software rather than defining a hardware solution. VLANs combine user stations and network devices into a single domain regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs managed through software reduce the amount of time in which network changes are implemented.

VLANs have no minimum number of ports, and can be created per unit, per device, per stack, or any other logical connection combination, as VLANs are software based and not defined by physical attributes.

VLANs function at layer 2. Since VLANs isolate traffic within the VLAN, a Layer 3 router is needed to allow traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs.

VLANs are broadcast and multicast domains. Broadcast and multicast traffic is transmitted only in the VLAN in which the traffic is generated.

The RVS4000 supports up to 4 VLANs, including the default VLAN.

L2 Switch > Create VLAN

VLAN ID The VLAN ID number. This can be any number from 2 to 3290, or from 3293 to 4094. (VLAN ID 1 is reserved for the default VLAN, which is used for untagged frames received on the interface. VLAN IDs 3291-3292 are reserved and cannot be used.) To create a VLAN, enter the ID number and click **Add VLAN**.

VLAN ID Range To create multiple VLANs with a range of ID numbers, enter the starting and ending ID numbers and click **Add Range**.

Delete Selected VLAN To delete a VLAN, select it form the VLAN list and click **Delete Selected VLAN**.

L2 > VLAN Port Setting

L2 Switch > VLAN Port Setting

Port ID Displays the port number from **1** to **4**.

Mode Select the mode of the port, either **Trunk**, **Untagged**, or **Tagged**. The default is **Untagged**. In Trunk mode, incoming and outgoing frames can be either tagged or untagged; incoming untagged frames are tagged with the default PVID (Port VLAN ID). In Untagged mode, all incoming and outgoing frames are untagged. In Tagged mode, all incoming and outgoing frames must be tagged; all untagged frames are dropped.

PVID The Port VLAN ID (PVID) assigned to untagged frames received on the interface. The default is **1**. If the Mode is Tagged, the port will receive only tagged frames and so the port will have no PVID.

L2 > VLAN Membership

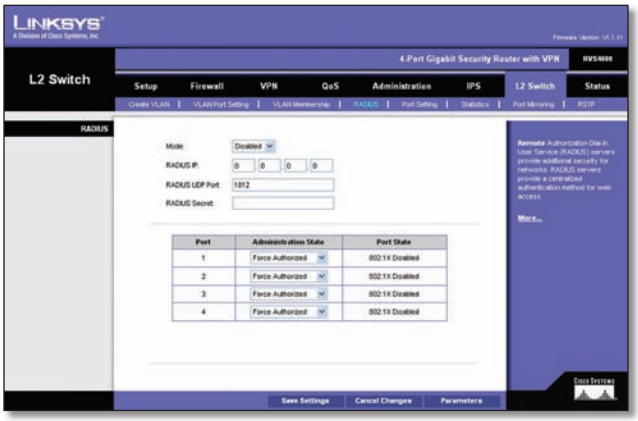
L2 Switch > VLAN Membership

VLAN ID Select the VLAN whose membership you want to configure.

Description Enter a VLAN group name of up to 50 characters.

Function/Port table The top half of the table indicates each port's current mode (Untagged, Tagged, or Trunk). The lower half of the table is used to assign port membership for the selected VLAN. The default for each port is **Exclude** (the port is not a member of the VLAN). To make a port a member of the VLAN, select the applicable mode(s). For example, if the port mode is Untagged, select Untagged; if the mode is Tagged, select Tagged; if the mode is Trunk, select either Tagged or Untagged.

L2 > RADIUS



L2 Switch > RADIUS

Mode Select **Enabled** or **Disabled** from the drop-down menu to enable or disable RADIUS.

RADIUS IP Enter the Server IP address.

RADIUS UDP Port Enter the UDP port. The UDP port is used to verify the RADIUS server authentication.

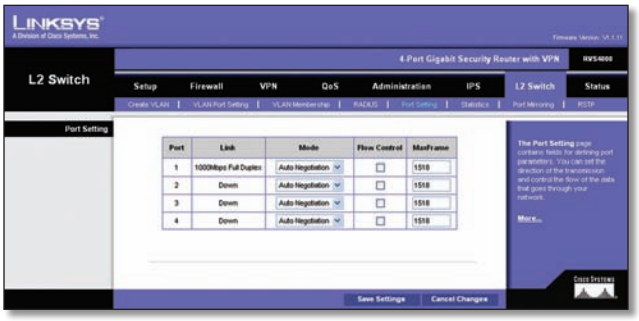
RADIUS Secret Enter the Key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS server encryption key. If no host-specific value is specified, the global value applies to each host.

Administration State Specifies the port authorization state. The possible field values are:

- **Auto** The controlled port state is set by the Authentication method.
- **Force Authorized** The controlled port state is set to Force-Authorized (forward traffic).
- **Force Unauthorized** The controlled port state is set to Force-Unauthorized (discard traffic).

Port State Displays the state of the selected port.

L2 > Port Setting



L2 Switch > Port Setting

Port Displays the physical port number.

Link Displays the port duplex mode and speed. **Full Duplex** indicates that the interface supports transmission between the device and its link partner in both directions simultaneously. **Half Duplex** indicates that the interface supports transmission between the device and the client in only one direction at a time.

Mode Select the port duplex mode and speed from the drop-down menu. You can also select **Auto Negotiation**, which is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.

Flow Control Displays the flow control status on the port. Operates when port is in Full duplex mode.

MaxFrame Displays the maximum frame size the port can receive and send.

L2 > Statistics

L2 Switch > Statistics

Statistics Overview

Tx Bytes Displays the number of Bytes transmitted from the selected port.

Tx Frames Displays the number of Frames transmitted from the selected port.

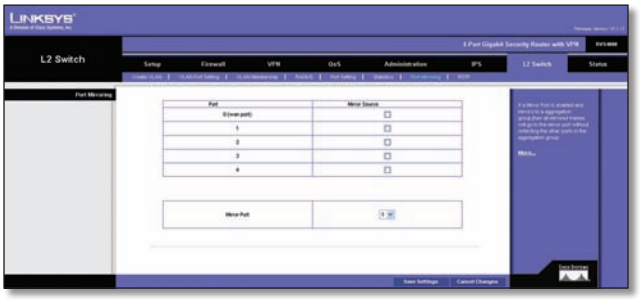
Rx Bytes Displays the number of Bytes received on the selected port.

Rx Frames Displays the number of Frames received on the selected port.

Tx Errors Displays the number of error packets transmitted from the selected port.

Rx Errors Displays the number of error packets received from the selected port.

L2 > Port Mirroring

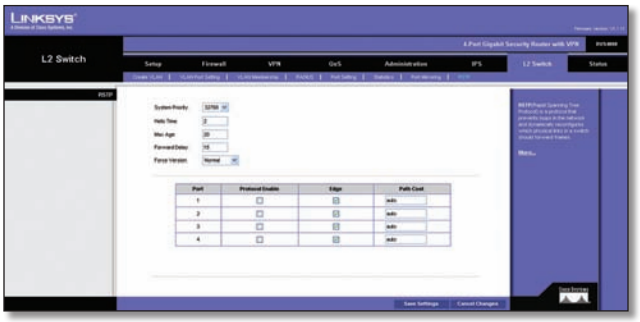


L2 Switch > Port Mirroring

Mirror Source Use this to enable or disable source port mirroring for each port on the Router. To enable source port mirroring on a port, check the box next to that port. To disable source port mirroring on a port, leave the box unchecked. The default is **disabled**.

Mirror Port Select the mirror destination port from the drop-down menu.

L2 > RSTP



L2 Switch > RSTP

The RSTP (Rapid Spanning Tree Protocol) protocol prevents loops in the network and dynamically reconfigures which physical links in a switch should forward frames.

System Priority Enter the system priority from 0 to 61440 in increments of 4096. Valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 40960, 45056, 49152, 53248, 57344, and 61440. The lower the system priority, the more likely the Router is to become the root in the Spanning Tree. The default is **32768**.

Hello Time Enter a number from 1 to 10. The default is **2**.

Max Age Enter a number from 6 to 40. The default is **20**.

Forward Delay Enter a number from 4 to 30. The default is **15**.

Force Version This is the default protocol version to use. Select Normal (use RSTP) or Compatible (compatible with old STP). The default is **Normal**.

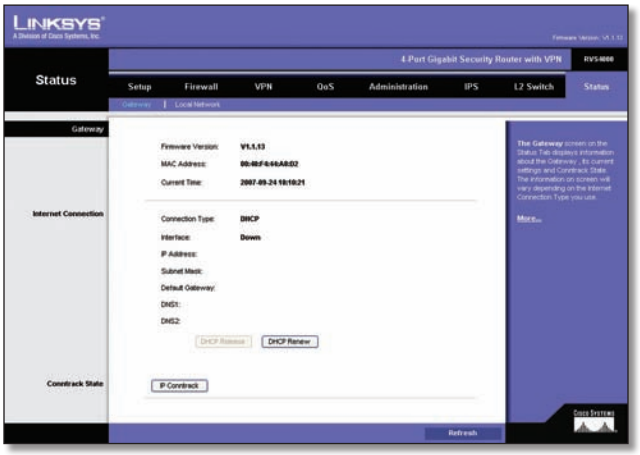
Protocol Enable Check this box to enable RSTP on the associated port. The default is unchecked (**RSTP disabled**).

Edge Check this box to specify that the associated port is an edge port (end station). Uncheck the box to specify that the associated port is a link (bridge) to another STP device. The default is checked (**edge port**).

Path Cost This is the RSTP path cost for the designated ports. Enter a number from 1 to 200000000, or auto (autogenerated path cost). The default is **auto**.

Status

Status > Gateway



Status > Gateway

Firmware Version Displays the Gateway's current firmware.

MAC Address Displays the Gateway MAC Address, as seen by your ISP.

Current Time Displays the time, based on the time zone you selected on the Setup tab.

Internet Connection

Connection Type Displays the type of the connection.

Interface Displays the Gateway Internet Interface.

IP Address Displays the Gateway Internet IP Address.

Subnet Mask Displays the Subnet Mask that is associated with the IP address above.

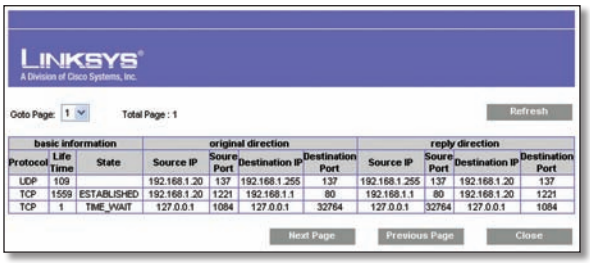
Default Gateway Displays your ISP's Gateway.

DNS 1-2 Displays the DNS (Domain Name System) IP addresses currently used by this Gateway.

IP Conntrack Click this button to display the IP Conntrack screen.

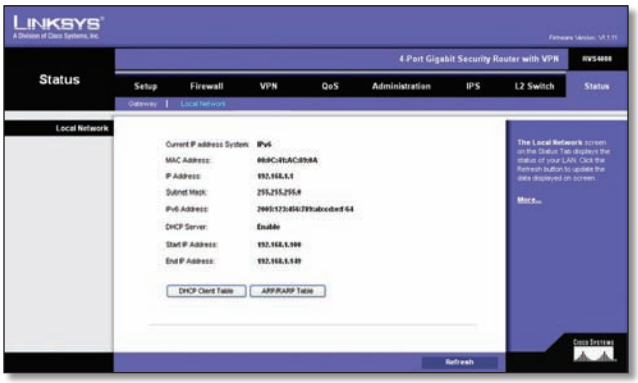
IP Conntrack

The IP Conntrack (Connection Tracking) screen displays information about TCP/UDP connections, such as source and destination IP address and port number pairs (known as socket pairs), protocol types (TCP/UDP/ICMP), connection state and timeouts. To see more information, click **Next Page** or **Previous Page**, or select the page from the *Goto Page* drop-down menu. To see the latest information, click **Refresh**. Click **Close** to return to the *Status > Gateway* screen.



Status > Gateway > IP Conntrack

Status > Local Network



Status > Local Network

Current IP address System This shows the current system.

MAC Address This is the Router MAC Address, as seen on your local, Ethernet network.

IP Address The Internet IP Address is displayed here.

Subnet Mask This Subnet Mask is associated with the IP address above.

IPv6 Address This shows the IPv6 IP address, if applicable.

DHCP Server The status of the Router's DHCP server function is displayed here.

Start IP Address This shows the beginning of the range of IP addresses used by the DHCP Server.

End IP Address This shows the end of the range of IP addresses used by the DHCP Server.

DHCP Client Table Clicking this button will open a screen showing you which PCs are utilizing the Router as a DHCP server. On the DHCP Client Table screen, you will see a list of DHCP clients (PCs and other network devices) with the following information: Client Names, Interfaces, IP Addresses, MAC Addresses, and the length of time before their assigned IP addresses expire.

ARP/RARP Table Clicking this button will open a screen showing you which PCs are utilizing the Router as an ARP/RARP server. On the ARP/RARP Table screen, you will see a list of ARPs/RARPs (PCs and other network devices) with the following information: IP Addresses and MAC Addresses.

Appendix A: Troubleshooting

This appendix provides solutions to problems that may occur during the installation and operation of the Router. Read the descriptions below to help solve your problems. If you can't find an answer here, check the Linksys website at www.linksys.com.

I need to set a static IP address on a PC.

The Router, by default, assigns an IP address range of 192.168.1.100 to 192.168.1.149 using the DHCP server on the Router. To set a static IP address, you can only use the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.150 to 192.168.1.254. Each PC or network device that uses TCP/IP must have a unique address to identify itself in a network. If the IP address is not unique to a network, Windows will generate an IP conflict error message. You can assign a static IP address to a PC by performing the following steps:

Windows 98 and Millennium

1. Click **Start**, **Setting**, and **Control Panel**. Double-click **Network**.
2. In *The following network components are installed* box, select the **TCP/IP->** associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click **Properties**.
3. In the *TCP/IP properties* window, click the **IP address** tab, and select **Specify an IP address**. Enter a unique IP address that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254. Make sure that each IP address is unique for each PC or network device.
4. Click the **Gateway** tab, and in the *New Gateway* field, enter **192.168.1.1**, which is the Router's default IP address. Click **Add** to accept the entry.
5. Click the **DNS** tab, and make sure the **DNS Enabled** option is selected. Enter the Host and Domain names (e.g., John for Host and home for Domain). Enter the DNS entry provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
6. Click **OK** in the *TCP/IP properties* window, and click **Close** or **OK** for the Network window.
7. Restart the computer when asked.

Windows 2000

1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
2. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and click **Properties**.
3. In the *Components checked are used by this connection* box, select **Internet Protocol (TCP/IP**), and click **Properties**. Select **Use the following IP address**.
4. Enter a unique IP address that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
5. Enter the Subnet Mask, **255.255.255.0**.
6. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
7. Select **Use the following DNS server addresses**, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
8. Click **OK** in the *Internet Protocol (TCP/IP) Properties* window, and click **OK** in the *Local Area Connection Properties* window.
9. Restart the computer if asked.

Windows XP

1. Click **Start** and **Control Panel**.
2. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
3. Right-click the **Local Area Connection** associated with your Ethernet adapter, and click **Properties**.
4. In the *This connection uses the following items* box, select **Internet Protocol (TCP/IP)**. Click **Properties**.
5. Select **Use the following IP address**, and enter a unique IP address that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
6. Enter the Subnet Mask, **255.255.255.0**.
7. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
8. Select **Use the following DNS server addresses**, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
9. Click **OK** in the *Internet Protocol (TCP/IP) Properties* window. Click **OK** in the *Local Area Connection Properties* window.

I want to test my Internet connection.

1. Check your TCP/IP settings.

   Windows 98 and Millennium

   Refer to Windows Help for details. Make sure **Obtain IP address automatically** is selected in the settings.

   Windows 2000

   a. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.

   b. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and click **Properties**.

   c. In the *Components checked are used by this connection* box, select **Internet Protocol (TCP/IP)**, and click **Properties**. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.

   d. Click **OK** in the *Internet Protocol (TCP/IP) Properties* window, and click **OK** in the *Local Area Connection Properties* window.

   e. Restart the computer if asked.

   Windows XP

   The following instructions are for the default interface of Windows XP. If you are using the Classic interface (the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

   a. Click **Start** and **Control Panel**.

   b. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.

   c. Right-click the **Local Area Connection** associated with your Ethernet adapter, and click **Properties**.

   d. In the *This connection uses the following items* box, select **Internet Protocol (TCP/IP)** and click **Properties**. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.

2. Open a command prompt:

   a. Windows 98 and Millennium: Click **Start** and **Run**. In the *Open* field, type **command**. Press **Enter** or click **OK**.

   b. Windows 2000 and XP: Click **Start** and **Run**. In the *Open* field, type **cmd**. Press **Enter** or click **OK**.

3. At the command prompt, type **ping 192.168.1.1** and press **Enter**.

   - If you get a reply, the computer is communicating with the Router.
   - If you do NOT get a reply, check the cable, and make sure **Obtain an IP address automatically** is selected in the TCP/IP settings for your Ethernet adapter.

4. At the command prompt, type **ping** followed by your Internet IP address and press **Enter**. The Internet IP Address can be found in the web interface of the Router. For example, if your Internet IP address is 1.2.3.4, you would enter **ping 1.2.3.4** and press **Enter**.

   - If you get a reply, the computer is connected to the Router.
   - If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

5. At the command prompt, type **ping www.linksys.com** and press **Enter**.

   - If you get a reply, the computer is connected to the Internet. If you cannot open a web page, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
   - If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

I am not getting an IP address on the Internet with my Internet connection.

1. Refer to "I want to test my Internet connection" above to verify that you have connectivity.
2. If you need to clone the MAC address of your Ethernet adapter onto the Router, see the MAC Address Clone section of "Chapter 5: Setting Up and Configuring the Router" for details.
3. Make sure you are using the right Internet settings. Contact your ISP to see if your Internet connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Basic Setup section of "Chapter 5: Setting Up and Configuring the Router" for details on Internet Connection Type settings.
4. Make sure you use the right cable. Check to see if the Internet LED is solidly lit.
5. Make sure the cable connecting from your cable or DSL modem is connected to the Router's Internet port. Verify that the Status page of the Router's Web-based Utility shows a valid IP address from your ISP.
6. Turn off the computer, Router, and cable/DSL modem. Wait 30 seconds, and then turn on the Router, cable/DSL modem, and computer. Check the System Summary tab of the Router's Web-based Utility to see if you get an IP address.

I am not able to access the Router's Web-based Utility Setup page.

1. Refer to "I want to test my Internet connection" above to verify that your computer is properly connected to the Router.
2. Verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
3. Set a static IP address on your system; refer to "I need to set a static IP address" above.
4. Refer to "I need to remove the proxy settings or the dial-up pop-up window (for PPPoE users)" below.

I can't get my Virtual Private Network (VPN) to work through the Router.

Access the Router's web interface by going to **http://192.168.1.1** or the IP address of the Router, and go to the **VPN -> VPN Pass Through** tab. Make sure you have IPSec passthrough and/or PPTP passthrough enabled.

VPNs that use IPSec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.

VPNs that use IPSec and AH (Authentication Header known as protocol 51) are incompatible with the Router. AH has limitations due to occasional incompatibility with the NAT standard.

Change the IP address for the Router to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Router will have difficulties routing information to the right location. If you change the Router's IP address to 192.168.2.1, that should solve the problem. Change the Router's IP address through the Setup tab of the Web-based Utility. If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.

Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPSec server. Refer to "I need to set up online game hosting or use other Internet applications" below for details.

Check the Linksys website at www.linksys.com for more information.

I need to set up a server behind my Router.

To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed. Follow these steps to set up port forwarding through the Router's Web-based Utility. We will be setting up web, ftp, and mail servers.

1. Access the Router's Web-based Utility by going to **http://192.168.1.1** or the IP address of the Router. Go to the **Firewall -> Single Port Forwarding** tab.
2. Select the Service from the *Application* column.
3. Enter the IP Address of the server that you want the Internet users to access. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Then check the **Enable** checkbox for the entry. Consider the examples below:

Appli-cation	Start and End	Proto-col	IP Address	Enable
HTTP	80 to 80	Both	192.168.1.100	X
FTP	21 to 21	TCP	192.168.1.101	X
SMTP (outgoing)	25 to 25	Both	192.168.1.102	X
POP3 (incoming)	110 to 110	Both	192.168.1.102	X

4. Configure as many entries as you like.

When you have completed the configuration, click **Save Settings**.

I need to set up online game hosting or use other Internet applications.

If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the Router to deliver incoming packets or data to a specific computer. This also applies to the Internet applications you are using. The best way to get the information on what port services to use is to go to the website of the online game or application you want to use. Follow these steps to set up online game hosting or use a certain Internet application:

1. Access the Router's Web-based Utility by going to **http://192.168.1.1** or the IP address of the Router. Go to the **Firewall -> Single Port Forwarding** tab.

2. Select the Service from the *Application* column.
3. Enter the IP Address of the server that you want the Internet users to access. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Then check the **Enable** checkbox for the entry. Consider the examples below:

Application	Start and End	Protocol	IP Address	Enable
UT	7777 to 27900	Both	192.168.1.100	X
Halflife	27015 to 27015	Both	192.168.1.105	X
PC Anywhere	5631 to 5631	UDP	192.168.1.102	X
VPN IPSEC	500 to 500	UDP	192.168.1.100	X

4. Configure as many entries as you like.

When you have completed the configuration, click **Save Settings**.

I can't get an Internet game, server, or application to work.

If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one PC to the Internet using DeMilitarized Zone (DMZ) hosting. This option is available when an application requires too many ports or when you are not sure which port services to use. Make sure you disable all the forwarding entries if you want to successfully use DMZ hosting, since forwarding has priority over DMZ hosting. (In other words, data that enters the Router will be checked first by the forwarding settings. If the port number that the data enters from does not have port forwarding, then the Router will send the data to whichever PC or network device you set for DMZ hosting.) Follow these steps to set DMZ hosting:

1. Access the Router's Web-based Utility by going to **http://192.168.1.1** or the IP address of the Router. Go to the **Firewall -> Single Port Forwarding** tab.
2. Disable the entries you have entered for forwarding.
3. Go to the **Setup -> DMZ** tab.
4. Enter the Ethernet adapter's IP address of the computer you want exposed to the Internet. This will bypass the NAT security for that computer.
5. Select **Enable** to enable DMZ Hosting.

When you have completed the configuration, click **Save Settings**.

I forgot my password, or the password prompt always appears when saving settings to the Router.

Reset the Router to factory defaults by pressing the Reset button for ten seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:

1. Access the Router's web interface by going to http://192.168.1.1 or the IP address of the Router. Enter the default password **admin**, and click the **Administration -> Management** tab.
2. Enter the old password in the *Old Password* field.
3. Enter a different password in the *New Password* field, and enter the new password in the *Confirm New Password* field to confirm the password.
4. Click **Save Settings**.

I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window.

If you have proxy settings, you need to disable these on your computer. Because the Router is the gateway for the Internet connection, the computer does not need any proxy settings to gain access. Please follow these directions to verify that you do not have any proxy settings and that the browser you use is set to connect directly to the LAN.

For Microsoft Internet Explorer 5.0 or higher:

1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Internet Options**.
2. Click the **Connections** tab.
3. Click **LAN settings** and remove anything that is checked.
4. Click **OK** to go back to the previous screen.
5. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.

For Netscape 4.7 or higher:

1. Start **Netscape Navigator**, and click **Edit**, **Preferences**, **Advanced**, and **Proxies**.
2. Make sure you have **Direct connection to the Internet** selected on this screen.
3. Close all the windows to finish.

To start over, I need to set the Router to factory default.

Hold the Reset button for up to 30 seconds and then release it. This will return the password, forwarding, and other settings on the Router to the factory default settings. In other words, the Router will revert to its original factory configuration.

I need to upgrade the firmware.

In order to upgrade the firmware with the latest features, you need to go to the Linksys website and download the latest firmware at www.linksys.com. Follow these steps:

1. Go to the Linksys website at **www.linksys.com** and download the latest firmware. Go to System Management -> Firmware Upgrade, and click **Firmware Download from Linksys Web Site**. Select the Router from the pull-down menu and choose the firmware from the options.
2. Extract the firmware file on your computer.
3. To upgrade the firmware, follow the steps in the Upgrade section found in "Chapter 5: Setting Up and Configuring the Router".

The firmware upgrade failed.

The upgrade could have failed for a number of reasons. Use the Linksys *RVS4000 Firmware Rescue Utility* to upgrade the firmware. Follow these steps to upgrade the firmware:

1. Go to the Linksys website at http://www.linksys.com and download *RVS4000 Firmware Rescue Utility v1.2*, which will be listed with the firmware. Save the zip file to your computer.
2. Extract the file **setup.exe** from the zip file, then run **setup.exe** to install the utility on your computer.
3. Disconnect the network cables from **all** of the Router's LAN and WAN ports, **except** the network cable to the computer that has the firmware upgrade utility.
4. Run the utility by clicking **Start**, **All Programs**, **Linksys**, **RVS4000 Upgrade Utility**, **RVS4000 Upgrade Utility**, or by double-clicking the icon on your desktop.
5. Follow the on-screen instructions to perform the upgrade.

My DSL service's PPPoE is always disconnecting.

PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet. There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.

1. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the Router.
2. Enter the password, if asked (default password is **admin**).
3. On the **Setup -> WAN** tab, select the option **Keep Alive**, and set the *Redial Period* option at **20** (seconds).
4. Click **Save Settings**.

If the connection is lost again, follow steps 1 and 2 to re-establish connection.

I can't access my email, web, or VPN, or I am getting corrupted data from the Internet.

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. For most DSL users, it is strongly recommended to use MTU 1492. If you are having difficulties, perform the following steps:

1. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the Router.
2. Enter the password, if asked (the default password is **admin**).
3. Go to the **Setup -> WAN** tab.
4. Look for the MTU option, and select **Manual**. In the *Size* field, enter **1492**.
5. Click **Save Settings** to continue.

If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved:

1462
1400
1362
1300

I need to use port triggering.

Port triggering looks at the outgoing port services used and will trigger the Router to open a specific port, depending on which port an Internet application uses. Follow these steps:

1. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the Router.
2. Enter the password, if asked (the default password is **admin**).
3. Click the **Firewall -> Port Range Triggering** tab.
4. Enter any name you want to use for the Application Name.
5. Enter the Start and End Ports of the Triggered Range. Check with your Internet application provider for more information on which outgoing port services it is using.
6. Enter the Start and End Ports of the Forwarded Range. Check with your Internet application provider for more information on which incoming port services are required by the Internet application.

7. Check the **Enabled** checkbox for the entry.

When you have completed the configuration, click **Save Settings**.

When I enter a URL or IP address, I get a time-out error or am prompted to retry.

- Check if other PCs work. If they do, ensure that your workstation's IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
- If the PCs are configured correctly, but still not working, check the Router. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)
- If the Router is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Router to verify a direct connection.
- Manually configure the TCP/IP with a DNS address provided by your ISP.
- Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

I'm trying to access the Router's Web-based Utility, but I do not see the login screen. Instead, I see a screen saying, "404 Forbidden."

If you are using Windows Explorer, perform the following steps until you see the Web-based Utility's login screen (Netscape Navigator will require similar steps):

1. Click **File**. Make sure **Work Offline** is NOT checked.
2. Press **CTRL + F5**. This is a hard refresh, which will force Windows Explorer to load new web pages, not cached ones.
3. Click **Tools**. Click **Internet Options**. Click the **Security** tab. Click the **Default level** button. Make sure the security level is Medium or lower. Then click the **OK** button.

I have QuickVPN tunnel connected to my RVS4000, but I cannot see the computers in the remote network from Windows Explorer.

QuickVPN tunneling does not support NetBIOS Broadcast. To access the computers or shared drives on the remote network, users are advised to use the IP address to identify the resource.

I have a Gateway-to-Gateway IPSec VPN tunnel connected between two RVS4000 routers, but the users in one network cannot see the computers in the remote network from Windows Explorer.

The RVS4000 supports NetBIOS Broadcast over a Gateway-to-Gateway IPSec VPN tunnel. However, the administrator needs to enable this feature in the Advanced section of the *VPN > IPSec VPN* screen.

Frequently Asked Questions

What is the maximum number of IP addresses that the Router will support?

The Router will support up to 253 IP addresses.

Is IPSec Passthrough supported by the Router?

Yes, enable or disable IPSec Passthrough on the *VPN > VPN Pass Through* screen.

Where is the Router installed on the network?

In a typical environment, the Router is installed between the cable/DSL modem and the LAN. Plug the Router into the cable/DSL modem's Ethernet port.

Does the Router support IPX or AppleTalk?

No. TCP/IP is the only protocol standard for the Internet and has become the global standard for communications. IPX, a NetWare communications protocol used only to route messages from one node to another, and AppleTalk, a communications protocol used on Apple and Macintosh networks, can be used for LAN to LAN connections, but those protocols cannot connect from the Internet to the LAN.

What is Network Address Translation and what is it used for?

Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Router to be used with low cost Internet accounts, such as DSL or cable modems, when only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

Does the Router support any operating system other than Windows 98, Millennium, 2000, or XP?

Yes, but Linksys does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.

Does the Router support ICQ send file?

Yes, with the following fix: click ICQ menu => preference => connections tab=>, and check I am behind a firewall or proxy. Then set the firewall time-out to 80 seconds in the firewall setting. The Internet user can then send a file to a user behind the Router.

I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do?

If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 to 27900. If you want to use the UT Server Admin, forward another port (8080 usually works well but is used for remote admin; you may have to disable this), and then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the Router from your ISP.

Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?

It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

How do I get Half-Life: Team Fortress to work with the Router?

The default client port for Half-Life is 27005. The computers on your LAN need to have "+clientport 2700x" added to the HL shortcut command line; the x would be 6, 7, 8, and on up. This lets multiple computers connect to the same server. One problem: Version 1.0.1.6 won't let multiple computers with the same CD key connect at the same time, even if on the same LAN (not a problem with 1.0.1.3). As far as hosting games, the HL server does not need to be in the DMZ. Just forward port 27015 to the local IP address of the server computer.

How can I block corrupted FTP downloads?

If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.

The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the screen. What do I need to do?

Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control Panel in your Ethernet adapter's Advanced Properties tab.) Make sure that your proxy setting is disabled in the browser. Check our website at www.linksys.com for more information.

If all else fails in the installation, what can I do?

Reset the Router by holding down the Reset button for ten seconds. Reset your cable or DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the Linksys website, www.linksys.com.

How can I be notified of new Router firmware upgrades?

All Linksys firmware upgrades are posted on the Linksys website at www.linksys.com, where they can be downloaded for free. The Router's firmware can be upgraded using the Web-based Utility. If the Router's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use. Downloading a more current version of Router firmware will not enhance the quality or speed of your Internet connection, and may disrupt your current connection stability.

Will the Router function in a Macintosh environment?

Yes, but the Router's setup pages are accessible only through Internet Explorer 5.0 or Netscape Navigator 5.0 or higher for Macintosh.

I am not able to get the web configuration screen for the Router. What can I do?

You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.

What is DMZ Hosting?

Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you want to use DMZ Hosting.

If DMZ Hosting is used, does the exposed user share the public IP with the Router?

No.

Does the Router pass PPTP packets or actively route PPTP sessions?

The Router allows PPTP packets to pass through.

Is the Router cross-platform compatible?

Any platform that supports Ethernet and TCP/IP is compatible with the Router.

How many ports can be simultaneously forwarded?

Theoretically, the Router can establish 2,048 sessions at the same time, but you can only forward 30 ranges of ports.

Does the Router replace a modem? Is there a cable or DSL modem in the Router?

No, this version of the Router must work in conjunction with a cable or DSL modem.

Which modems are compatible with the Router?

The Router is compatible with virtually any cable or DSL modem that supports Ethernet.

How can I check whether I have static or DHCP IP addresses?

Ask your ISP to find out.

How do I get mIRC to work with the Router?

Under the **Firewall -> SIngle Port Forwarding** tab, set port forwarding to 113 for the PC on which you are using mIRC.

Appendix B: Using Linksys QuickVPN for Windows 2000, XP, or Vista

Overview

This appendix explains how to install and use the Linksys QuickVPN software that can be downloaded from www.linksys.com. QuickVPN works with computers running Windows 2000, XP, or Vista. (Computers using other operating systems will have to use third-party VPN software.) For Windows Vista, QuickVPN Client version 1.2.5 or later is required.

Before You Begin

The QuickVPN program only works with a Linksys 4-Port Gigabit Security Router with VPN that is properly configured to accept a QuickVPN connection. Follow these instructions to configure the Router's VPN client settings:

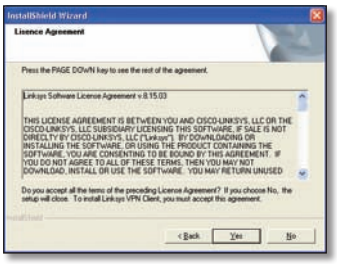
1. Click the **VPN** tab.
2. Click the **VPN Client Accounts** tab.
3. Enter the username in the *Username* field.
4. Enter the password in the *Password* field, and enter it again in the *Re-enter to confirm* field.
5. Click **Add/Save**.
6. Click the **Active** checkbox for VPN Client No. 1.
7. Click **Save Settings**.

VPN Client Accounts Screen

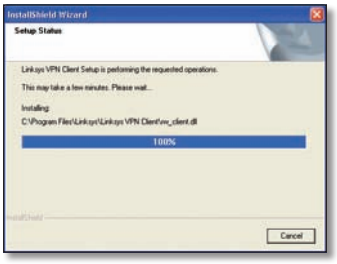
Installing the Linksys QuickVPN Software

Installing from the CD-ROM

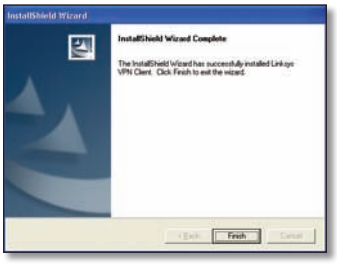
1. Insert the RVS4000 CD-ROM into your CD-ROM drive. Go to the **Start** menu and then click **Run**. In the field provided, enter **D:\VPN_Client.exe** (if "**D**" is the letter of your CD-ROM drive).
2. The License Agreement screen appears. Click **Yes** to accept the agreement and the appropriate files are copied to the computer.



License Agreement



Copying Files



Finished Installing Files

3. Click **Finished** to complete the installation. Proceed to the section, "Using the Linksys QuickVPN Software".

Downloading and Installing from the Internet

1. Go to **www.linksys.com** and select **Products**.
2. Click **Business Solutions**.
3. Click **Router/VPN Solutions**.
4. Click **RVS4000**.
5. Click **Linksys QuickVPN Utility** in the More Information section.

6. Save the zip file to your PC, and extract the .exe file.
7. Double-click the .exe file, and follow the on-screen instructions. Proceed to the next section, "Using the Linksys QuickVPN Software".

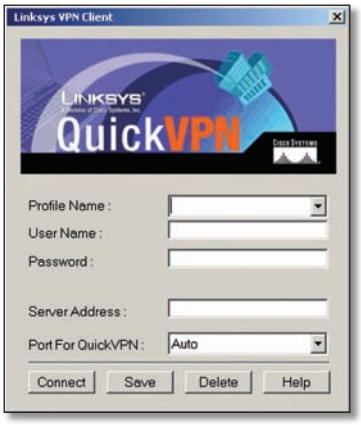
Using the Linksys QuickVPN Software

1. Double-click the Linksys QuickVPN software icon on your desktop or in the system tray.

QuickVPN Desktop Icon

QuickVPN Tray Icon—
No Connection

2. The QuickVPN Login screen will appear. In the *Profile Name* field, enter a name for your profile. In the *User Name* and *Password* fields, enter the User Name and Password that were assigned to you. In the *Server Address* field, enter the IP address or domain name of the Linksys 4-Port Gigabit Security Router with VPN. In the *Port For QuickVPN* field, enter the port number that the QuickVPN client will use to communicate with the remote VPN router, or keep the default setting, **Auto**.



QuickVPN Login

To save this profile, click **Save**. (If there are multiple sites to which you will need to create a tunnel, you can create multiple profiles, but note that only one tunnel can be active at a time.) To delete this profile, click **Delete**. For information, click **Help**.

3. To begin your QuickVPN connection, click **Connect**. The connection's progress is displayed: *Connecting*, *Provisioning*, *Activating Policy*, and *Verifying Network*.
4. When your QuickVPN connection is established, the QuickVPN tray icon turns green, and the QuickVPN Status screen appears. The screen displays the IP address of the remote end of the VPN tunnel, the time and date the VPN tunnel began, and the total length of time the VPN tunnel has been active.

QuickVPN Tray Icon—
Connection

QuickVPN Status

To terminate the VPN tunnel, click **Disconnect**. To change your password, click **Change Password**. For information, click **Help**.

5. If you clicked **Change Password** and have permission to change your own password, you will see the *Connect Virtual Private Connection* screen. Enter your password in the *Old Password* field. Enter your new password in the *New Password* field. Then enter the new password again in the *Confirm New Password* field. Click **OK** to save your new password. Click **Cancel** to cancel your change. For information, click **Help**.

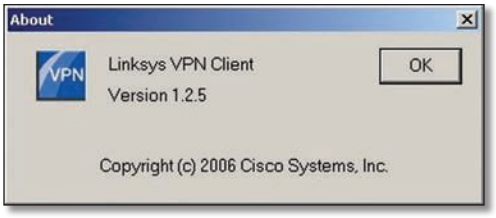
Connect Virtual Private Connection

NOTE: You can change your password only if you have been granted that privilege by your system administrator.

Version Number of the QuickVPN Client

To display the version number of the QuickVPN Client:

1. Right-click the QuickVPN tray icon, then select **About**.
2. The *About* screen displays the QuickVPN Client version number.
3. Click **OK** to close the *About* screen.



QuickVPN Client Version Number

Distributing Certificates to QuickVPN Users

The following explains how to export a certificate from the RVS4000 for distribution to QuickVPN users, as well as how to install the certificate on the QuickVPN users' PCs.

1. Generate the Certificate as follows:
   a. Log on to the Web-based Utility.
   b. Select **VPN**, then **VPN Client Accounts**.
   c. Click **Generate** to generate a new certificate.
   d. Click **Export for Client** and save the certificate as a **.PEM** file.
2. Distribute the certificate to all QuickVPN users.
3. Each QuickVPN user must then install the certificate as follows:
   a. Save the certificate into the directory where the QuickVPN Client is installed. For example: **C:\Program Files\Linksys\QuickVPN Client**
   b. Launch the QuickVPN Client and specify the User Name, Password, and Server Address (IP address or domain name).
   c. Click **Connect**.

For more information on certificate management, go to section "VPN > VPN Client Accounts" in "Chapter 5: Setting Up and Configuring the Router".

Appendix C: Configuring IPSec with a Windows 2000 or XP Computer

Introduction

This appendix explains how to establish a secure IPSec tunnel using preshared keys to join a private network inside the Router and a Windows 2000 or XP computer. You can find detailed information on configuring the Windows 2000 server at the Microsoft website:

Microsoft KB Q252735—How to Configure IPSec Tunneling in Windows 2000:
http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

Microsoft KB Q257225—Basic IPSec Troubleshooting in Windows 2000:
http://support.microsoft.com/support/kb/articles/Q257/2/25.asp

NOTE: Keep a record of any changes you make. Those changes will be identical in the Windows "secpol" application and the Router's Web-based Utility.

NOTE: The text on your screen may differ from the text in your instructions regarding the **OK** or **Close** buttons; click the appropriate button on your screen.

Environment

The IP addresses and other specifics mentioned in this appendix are for illustration purposes only.

Windows 2000 or Windows XP

IP Address: 140.111.1.2 <= User ISP provides IP Address; this is only an example.

Subnet Mask: 255.255.255.0

RVS4000

WAN IP Address: 140.111.1.1 <= User ISP provides IP Address; this is only an example.

Subnet Mask: 255.255.255.0

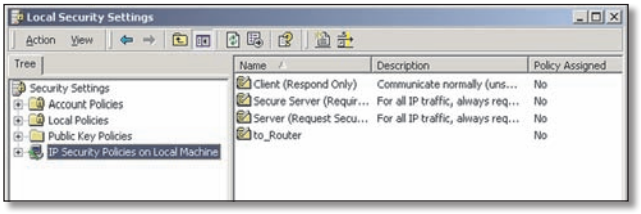
LAN IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

How to Establish a Secure IPSec Tunnel

Step 1: Create an IPSec Policy

1. Click **Start**, select **Run**, and type **secpol.msc** in the *Open* field. The Local Security Settings screen appears.



Local Security Settings

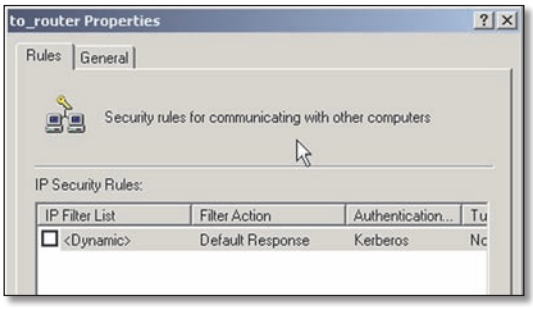
2. Right-click **IP Security Policies on Local Computer** (Windows XP) or **IP Security Policies on Local Machine** (Windows 2000), and click **Create IP Security Policy**.
3. Click the **Next** button, and then enter a name for your policy (for example, to_Router). Then, click **Next**.
4. Deselect the **Activate the default response rule** check box, and then click **Next**.
5. Click **Finish**, making sure the **Edit** check box is checked.

Step 2: Build Filter Lists

NOTE: Throughout the following section the term "win" refers to both Windows 2000 and Windows XP.

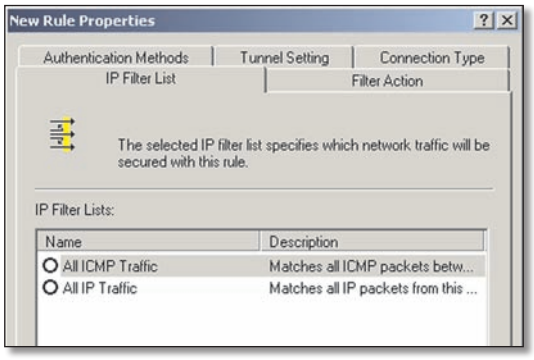
Filter List 1: win -> router

1. In the new policy's properties screen, verify that the **Rules** tab is selected. Deselect the **Use Add Wizard** check box, and click **Add** to create a new rule.



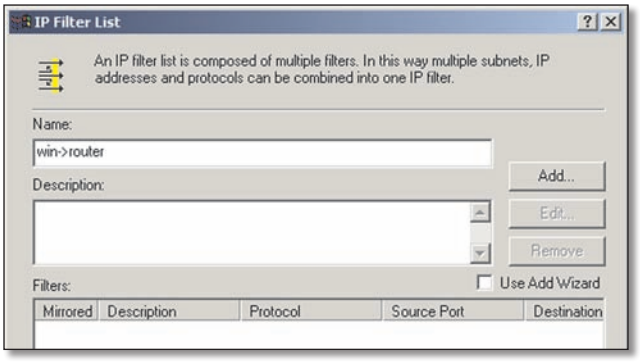
Rules Tab

2. Make sure the **IP Filter List** tab is selected. Click **Add**.



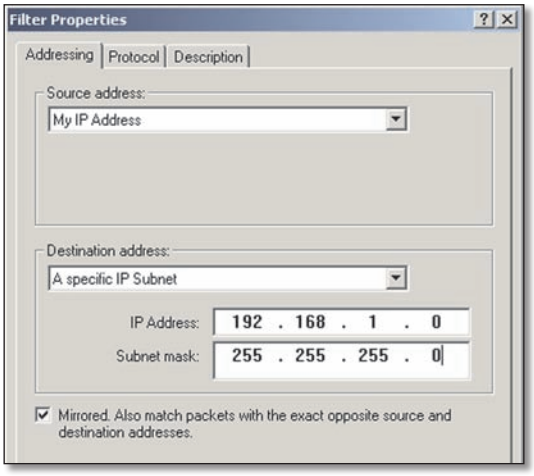
IP Filter List Tab

3. The *IP Filter List* screen should appear. Enter an appropriate name, such as win->Router, for the filter list, and de-select the **Use Add Wizard** check box. Then, click **Add**.



IP Filter List

4. The *Filters Properties* screen will appear. Select the **Addressing** tab.



Filters Properties

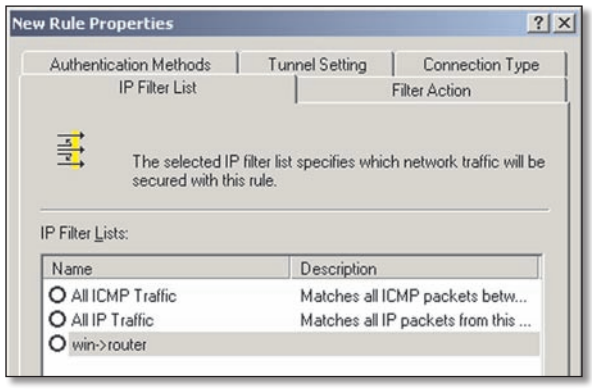
In the *Source address* field, select **My IP Address**. In the *Destination address* field, select **A specific IP Subnet**, and enter the IP Address **192.168.1.0** and Subnet mask **255.255.255.0**. (These are the Router's default settings. If you have changed these settings, enter your new values.)

5. If you want to enter a description for your filter, click the **Description** tab and enter the description there.

6. Click **OK**. Then, click **OK** or **Close** in the *IP Filter List* window.

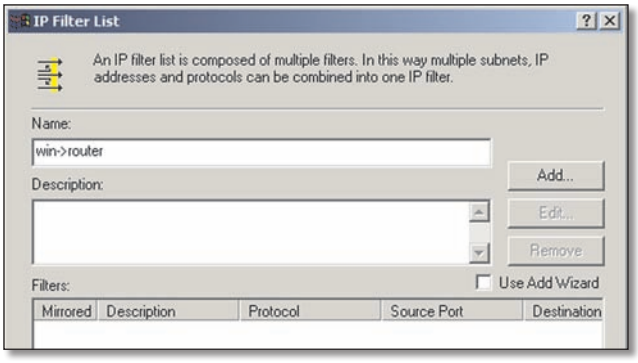
Filter List 2: router -> win

7. The *New Rule Properties* screen will appear. Select the **IP Filter List** tab, and make sure that **win -> Router** is highlighted. Then, click **Add**.



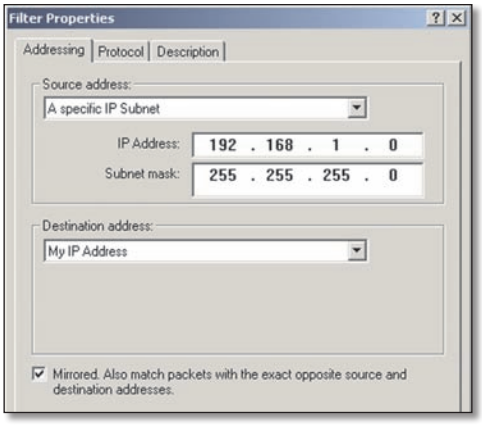
New Rules Properties

8. The *IP Filter List* screen should appear. Enter an appropriate name, such as **Router->win** for the filter list, and de-select the **Use Add Wizard** check box. Click **Add**.



IP Filter List

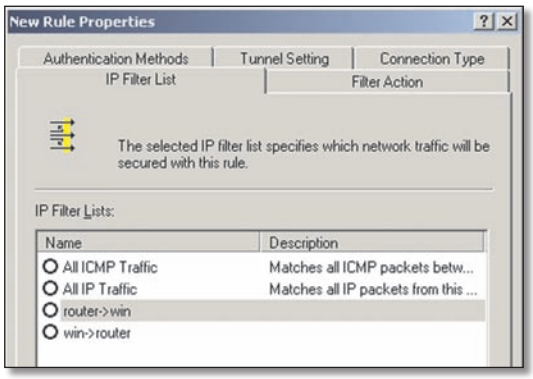
9. The *Filters Properties* screen will appear. Select the **Addressing** tab. In the **Source address** field, select **A specific IP Subnet**, and enter the IP Address **192.168.1.0** and Subnet mask **255.255.255.0**. (Enter your new values if you have changed the default settings.) In the *Destination address* field, select **My IP Address**.



Filters Properties

10. If you want to enter a description for your filter, click the **Description** tab and enter the description there.

11. Click **OK** or **Close** and the *New Rule Properties* screen appears with the **IP Filter List** tab selected. The screen will contain listings for **Router->win** and **win->Router**. Click **OK** (Windows XP) or **Close** (Windows 2000) in the *IP Filter List* window.

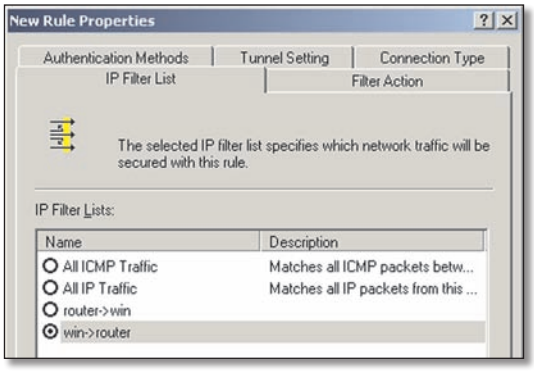


New Rule Properties

Step 3: Configure Individual Tunnel Rules

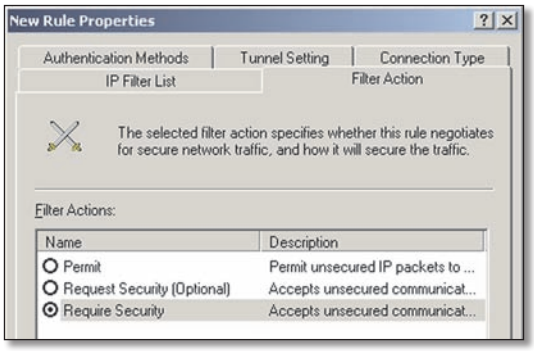
Tunnel 1: win->Router

1. On the **IP Filter List** tab, select filter list **win->Router**.



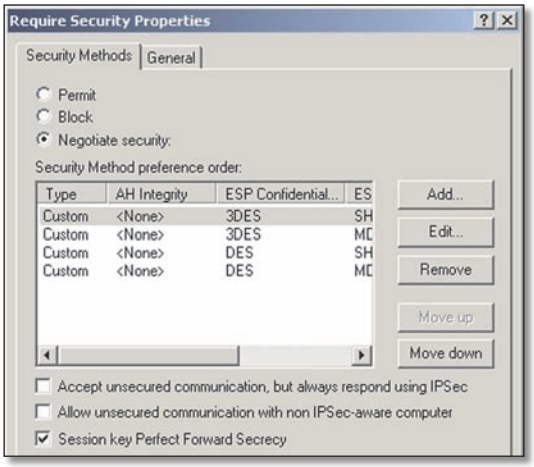
IP Filter List Tab

2. Click the *Filter Action* tab, and click the filter action **Require Security** radio button. Then, click **Edit**.



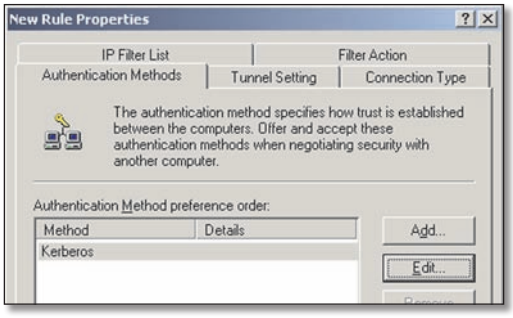
Filter Action Tab

3. On the *Security Methods* tab, verify that the **Negotiate security** option is enabled, and deselect the **Accept unsecured communication, but always respond using IPSec** check box. Select **Session key Perfect Forward Secrecy**, and click **OK**.



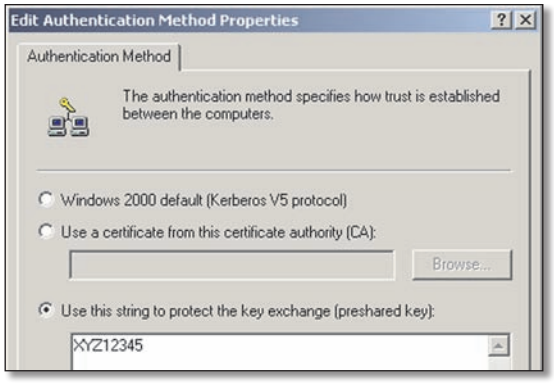
Security Methods Tab

4. Select the **Authentication Methods** tab, and click **Edit**.



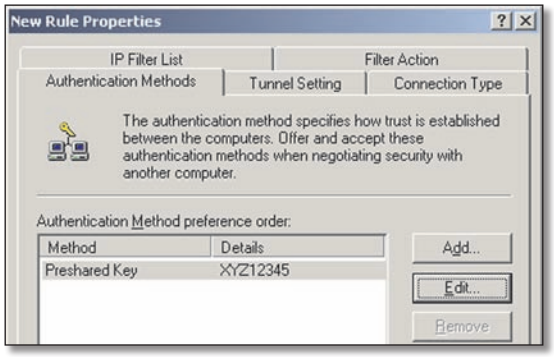
Authentication Methods Tab

5. Change the authentication method to **Use this string to protect the key exchange (preshared key)**, and enter the preshared key string, such as XYZ12345. Click **OK**.


Edit Authentication Method Properties
Authentication Method
The authentication method specifies how trust is established between the computers.
Windows 2000 default (Kerberos V5 protocol)
Use a certificate from this certificate authority (CA):
Browse...
Use this string to protect the key exchange (preshared key):
XYZ12345

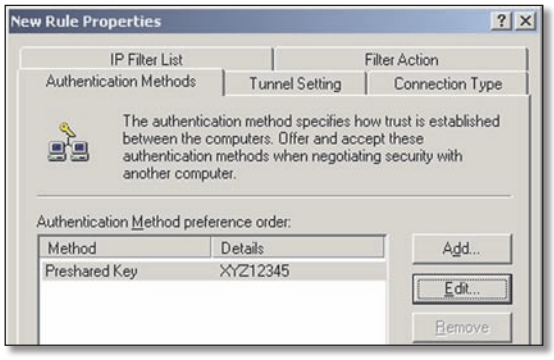
Preshared Key

6. This new Preshared key will be displayed. Click the **Apply** button to continue, if it appears on your screen; otherwise, proceed to the next step.



New Preshared Key

7. Select the **Tunnel Setting** tab, and click **The tunnel endpoint is specified by this IP Address** radio button. Then, enter the Router's WAN IP Address.



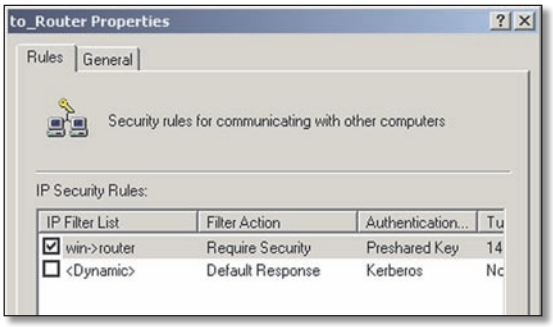
Tunnel Setting Tab

8. Select the **Connection Type** tab, and click **All network connections**. Then, click the **OK** or **Close** button to finish this rule.

Connection Type Tab

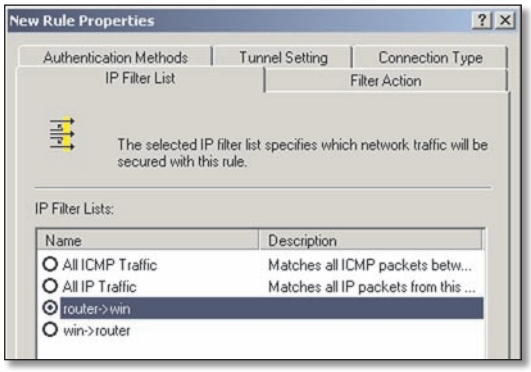
Tunnel 2: Router->win

9. In the new policy's Properties screen, make sure that **win -> Router** is selected and deselect the **Use Add Wizard** check box. Then, click **Add** to create the second IP filter.



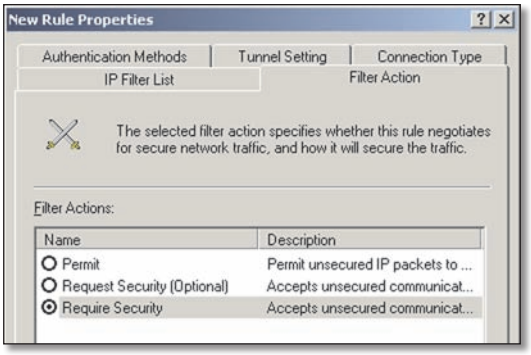
Properties Screen

10. Go to the **IP Filter List** tab, and click the filter list **Router->win**.



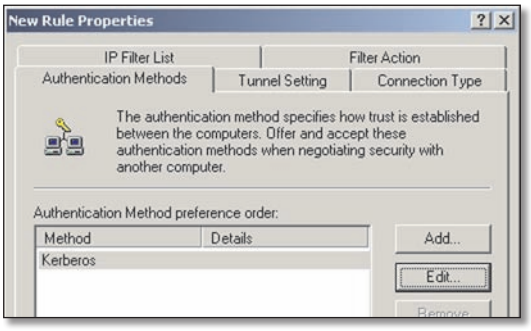
IP Filter List Tab

11. Click the **Filter Action** tab, and select the filter action **Require Security**. Then, click **Edit**. On the **Security Methods** tab, verify that the **Negotiate security** option is enabled, and deselect the **Accept unsecured communication, but always respond using IPSec** check box. Select **Session key Perfect Forward Secrecy**, and click **OK**.



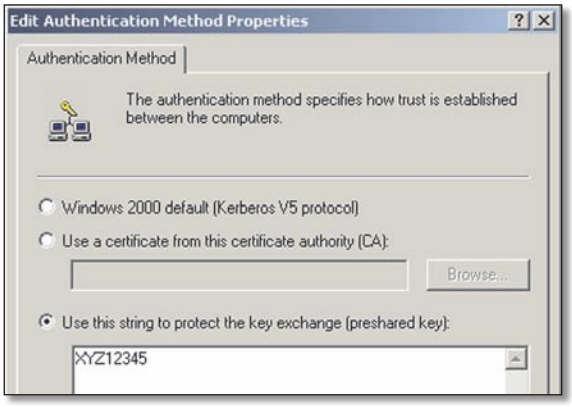
Filter Action Tab

12. Click the **Authentication Methods** tab, and verify that the authentication method **Kerberos** is selected. Then, click **Edit**.



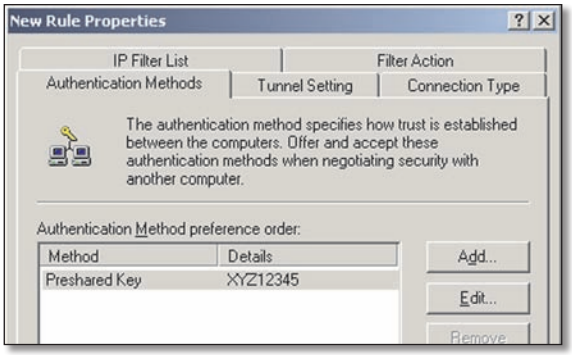
Authentication Methods Tab

13. Change the authentication method to **Use this string to protect the key exchange (preshared key)**, and enter the preshared key string, such as XYZ12345. (This is a sample key string. Yours should be a key that is unique but easy to remember.) Then click **OK**.


Edit Authentication Method Properties
Authentication Method
The authentication method specifies how trust is established between the computers.
Windows 2000 default (Kerberos V5 protocol)
Use a certificate from this certificate authority (CA):
Browse...
Use this string to protect the key exchange (preshared key):
XYZ12345

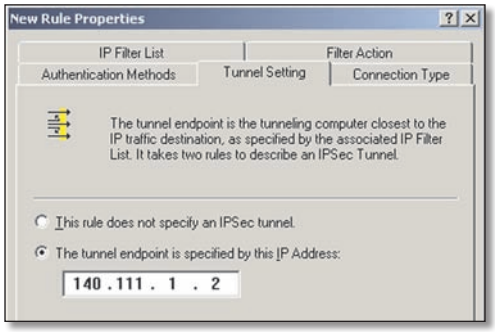
Preshared Key

14. This new Preshared key will be displayed. Click the **Apply** button to continue, if it appears on your screen; otherwise, proceed to the next step.



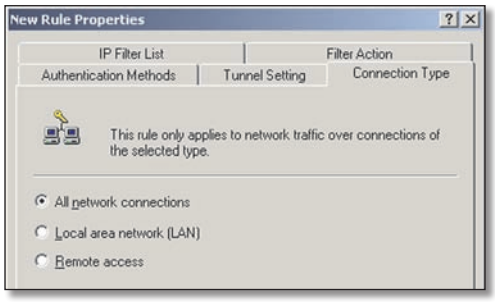
New Preshared Key

15. Click the **Tunnel Setting** tab. Click the radio button **The tunnel endpoint is specified by this IP Address**, and enter the Windows 2000/XP computer's IP Address.


New Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.
This rule does not specify an IPSec tunnel.
The tunnel endpoint is specified by this IP Address:
140 . 111 . 1 . 2

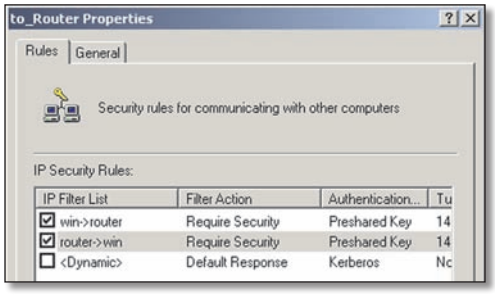
Tunnel Setting Tab

16. Click the **Connection Type** tab, and select **All network connections**. Then click **OK** or **Close** to finish.



Connection Type Tab

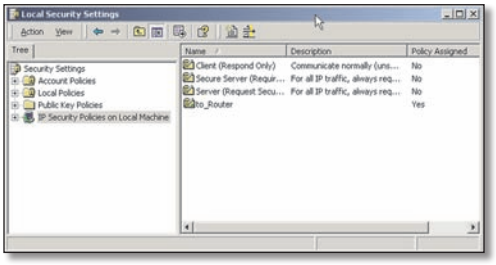
17. On the **Rules** tab, click the **OK** or **Close** button to return to the screen showing the security policies.



Rules Tab

Step 4: Assign New IPSec Policy

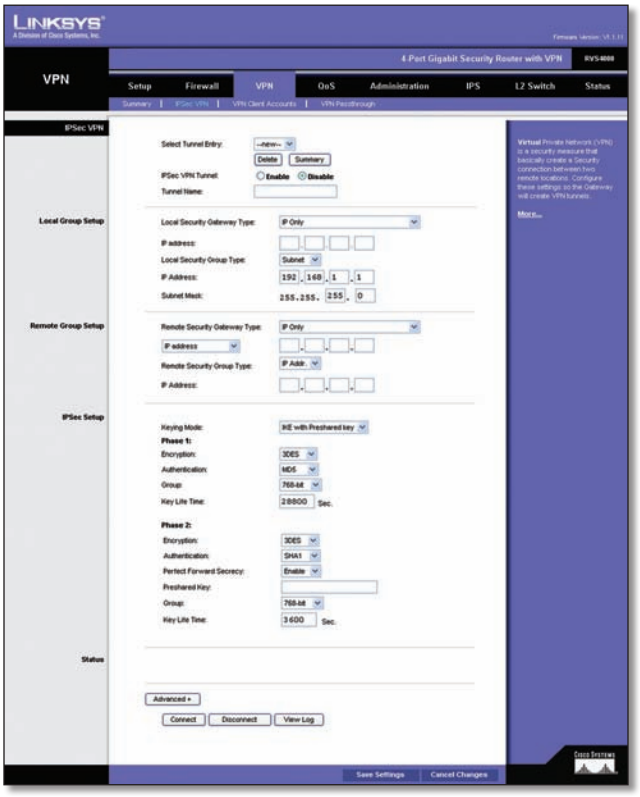
In the *IP Security Policies on Local Machine* window, right-click the policy named **to_Router**, and click **Assign**. A green arrow appears in the folder icon.



Local Computer

Step 5: Create a Tunnel Through the Web-Based Utility

1. Open your web browser, and enter **192.168.1.1** in the *Address* field. Press **Enter**.
2. When the *User name* and *Password* fields appear, enter the default user name and password, **admin**. Press **Enter**.
3. Click the **VPN** tab, then click **IPSec VPN**.



VPN > IPSec VPN

4. Select the tunnel you wish to create in the *Select Tunnel Entry* drop-down box. Then click **Enable**. Enter the name of the tunnel in the *Tunnel Name* field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.
5. Enter the IP Address and Subnet Mask of the local VPN Router in the *Local Group Setup* fields. To allow access to the entire IP subnet, enter **0** for the last set of IP Addresses (e.g. 192.168.1.0).
6. Enter the IP Address and Subnet Mask of the VPN device at the other end of the tunnel (the remote VPN Router or device with which you wish to communicate) in the *Remote Group Setup* fields.
7. Select from two types of authentication: **MD5** and **SHA1** (SHA1 is recommended because it is more secure). As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to **Disable** authentication.
8. Select the Key Management. Select **Auto (IKE)** and enter a series of numbers or letters in the *Pre-shared Key* field. Select **PFS** (Perfect Forward Secrecy) to ensure that the initial key exchange and IKE proposals are secure. You may use any combination of up to 128 numbers or letters in this field. No special characters or spaces are allowed. In the *Key Lifetime* field, you may optionally select to have the key expire at the end of a time period you designate. Enter the number of seconds you'd like the key to be useful, or leave it blank for the key to last indefinitely.
9. Click **Save Settings** to save these changes.

Your tunnel should now be established.

Appendix D: Gateway-to-Gateway VPN Tunnel

Overview

This appendix explains how to configure an IPSec VPN tunnel between two VPN Routers by example. Two computers are used to test the liveliness of the tunnel.

Before You Begin

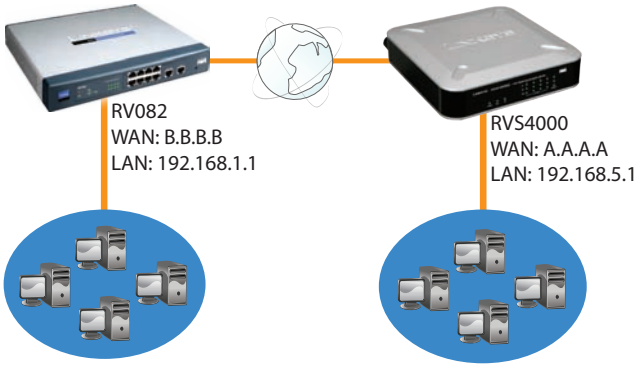
The following is a list of equipment you need:

- Two Windows desktop computers (each computer will be connected to a VPN Router)
- Two VPN Routers (4-Port Gigabit Security Router with VPN, model number RVS4000, and 10/100 8-Port VPN Router, model number RV082) that are both connected to the Internet

Any VPN Router can be deployed, such as the Linksys 10/100 16-, 8-, or 4-Port VPN Router (model numbers RV016, RV082, or RV042); however, this example uses the RV082.

Configuration when the Remote Gateway Uses a Static IP Address

This example assumes the Remote Gateway is using a static IP address. If the Remote Gateway uses a dynamic IP address, refer to "Configuration when the Remote Gateway Uses a Dynamic IP."



Gateway-to-Gateway IPSec VPN Tunnel - Remote Gateway Using Static IP

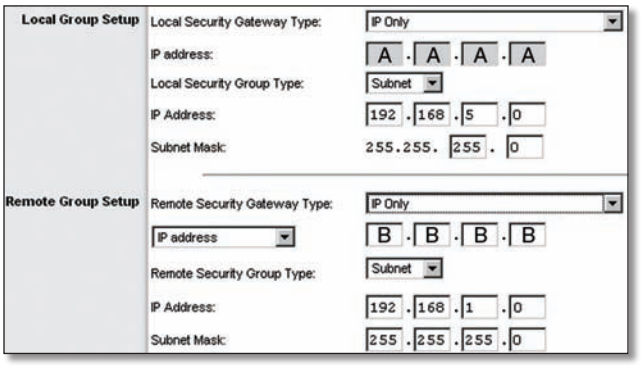
NOTE: Each computer must have a network adapter installed.

Configuration of the RVS4000

Follow these instructions for the first VPN Router, designated RVS4000. The other VPN Router is designated the RV082.

1. Launch the web browser for a networked computer, designated PC 1.
2. Access the web-based utility of the RVS4000. (Refer to "Chapter 5: Setting Up and Configuring the Router" for details.)
3. Click the **VPN** tab.
4. Click **IPSec VPN**.
5. Enter a name in the *Tunnel Name* field.
6. For the IPSec VPN Tunnel setting, select **Enable**.
7. The WAN IP address (A.A.A.A) of the RVS4000 will be automatically detected.

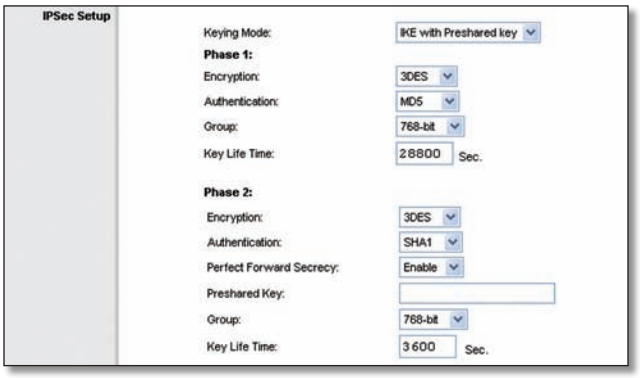
   For the Local Security Group Type, select **Subnet**. Enter the RVS4000's local network settings in the *IP Address* and *Subnet Mask* fields.


Local Group Setup
Local Security Gateway Type: IP Only
IP address: A . A . A . A
Local Security Group Type: Subnet
IP Address: 192 . 168 . 5 . 0
Subnet Mask: 255.255. 255 . 0
Remote Group Setup
Remote Security Gateway Type: IP Only
IP address B . B . B . B
Remote Security Group Type: Subnet
IP Address: 192 . 168 . 1 . 0
Subnet Mask: 255 . 255 . 255 . 0

RVS4000 IPSec VPN Settings

8. For the Remote Security Gateway Type, select **IP address**. Enter the RV082's WAN IP address in the *IP Address* field.
9. For the Remote Security Group Type, select **Subnet**. Enter the RV082's local network settings in the *IP Address* and *Subnet Mask* fields.

10. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings.
11. In the *Preshared Key* field, enter a string for this key, for example, 13572468.



RVS4000 IPSec Setup Settings

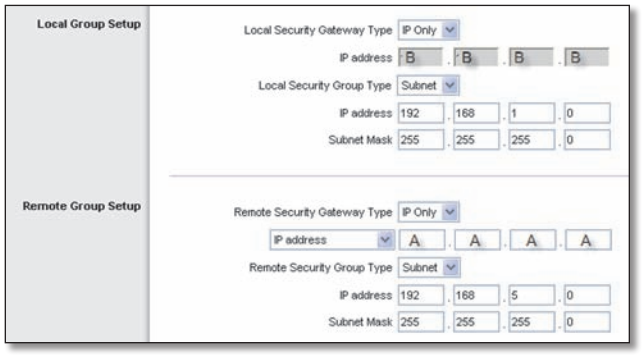
12. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save Settings** and proceed to the next section, "Configuration of the RV082."

Configuration of the RV082

Follow similar instructions for the RV082.

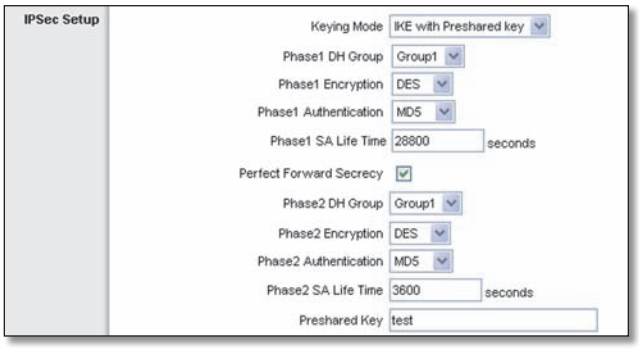
1. Launch the web browser for a networked computer, designated PC 2.
2. Access the web-based utility of the RV082. (Refer to the User Guide of the RV082 for details.)
3. Click the **IPSec VPN** tab.
4. Click the **Gateway to Gateway** tab.
5. Enter a name in the *Tunnel Name* field.
6. For the VPN Tunnel setting, select **Enable**.
7. The WAN IP address (B.B.B.B) of the RV082 will be automatically detected.

   For the Local Security Group Type, select **Subnet**. Enter the RV082's local network settings in the *IP Address* and *Subnet Mask* fields.


Local Group Setup
Local Security Gateway Type IP Only
IP address B . B . B . B
Local Security Group Type Subnet
IP address 192 . 168 . 1 . 0
Subnet Mask 255 . 255 . 255 . 0
Remote Group Setup
Remote Security Gateway Type IP Only
IP address A . A . A . A
Remote Security Group Type Subnet
IP address 192 . 168 . 5 . 0
Subnet Mask 255 . 255 . 255 . 0

RV082 VPN Settings

8. For the Remote Security Gateway Type, select **IP address**. Enter the RVS4000's WAN IP address in the *IP Address* field.
9. For the Remote Security Group Type, select **Subnet**. Enter the RVS4000's local network settings in the *IP Address* and *Subnet Mask* fields.
10. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings. (These should match the settings of the RVS4000.)
11. In the *Preshared Key* field, enter a string for this key, for example, 13572468.



RV082 IPSec Setup Settings

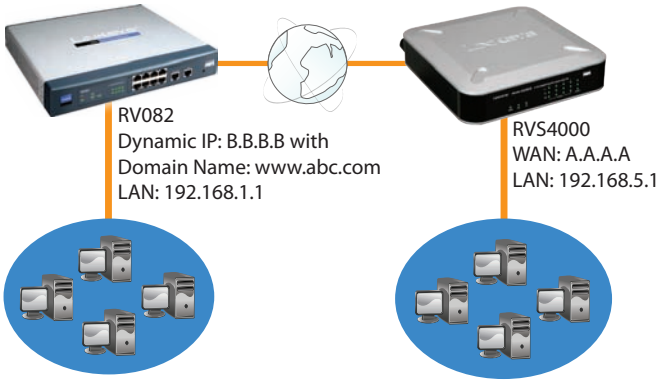
12. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save Settings**.

Configuration of PC 1 and PC 2

Verify that PC 1 and PC 2 can ping each other (refer to Windows Help for more information). If the computers can ping each other, then you know the VPN tunnel is configured correctly.

Configuration when the Remote Gateway Uses a Dynamic IP Address

This example assumes the Remote Gateway is using a dynamic IP address. If the Remote Gateway uses a static IP address, refer to "Configuration when the Remote Gateway Uses a Static IP."



Gateway-to-Gateway IPSec VPN Tunnel - Remote Gateway Using Dynamic IP

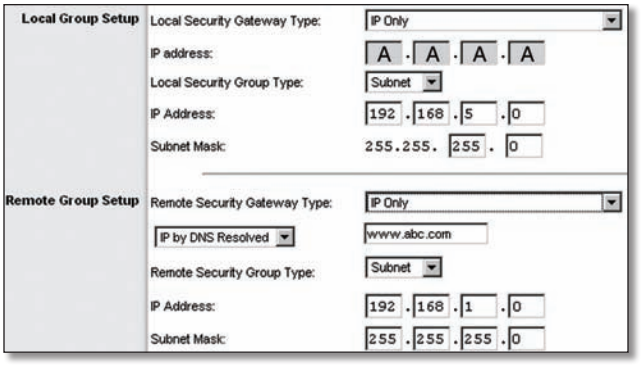
NOTE: Each computer must have a network adapter installed.

Configuration of the RVS4000

Follow these instructions for the first VPN Router, designated RVS4000. The other VPN Router is designated the RV082.

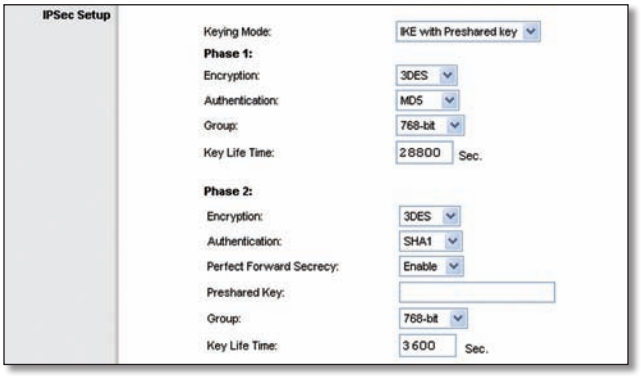
1. Launch the web browser for a networked computer, designated PC 1.
2. Access the web-based utility of the RVS4000. (Refer to "Chapter 5: Setting Up and Configuring the Router" for details.)
3. Click the **VPN** tab.
4. Click **IPSec VPN**.
5. Enter a name in the *Tunnel Name* field.
6. For the IPSec VPN Tunnel setting, select **Enable**.
7. The WAN IP address (A.A.A.A) of the RVS4000 will be automatically detected.

   For the Local Security Group Type, select **Subnet**. Enter the RVS4000's local network settings in the *IP Address* and *Subnet Mask* fields.


Local Group Setup
Local Security Gateway Type: IP Only
IP address: A . A . A . A
Local Security Group Type: Subnet
IP Address: 192 . 168 . 5 . 0
Subnet Mask: 255.255. 255 . 0
Remote Group Setup
Remote Security Gateway Type: IP Only
IP by DNS Resolved www.abc.com
Remote Security Group Type: Subnet
IP Address: 192 . 168 . 1 . 0
Subnet Mask: 255 . 255 . 255 . 0

RVS4000 IPSec VPN Settings

8. For the Remote Security Gateway Type, select **IP by DNS Resolved**. Enter the RV082's domain name in the field provided.
9. For the Remote Security Group Type, select **Subnet**. Enter the RV082's local network settings in the *IP Address* and *Subnet Mask* fields.
10. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings.
11. In the *Preshared Key* field, enter a string for this key, for example, 13572468.



RVS4000 IPSec Setup Settings

12. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save Settings** and proceed to the next section, "Configuration of the RV082."

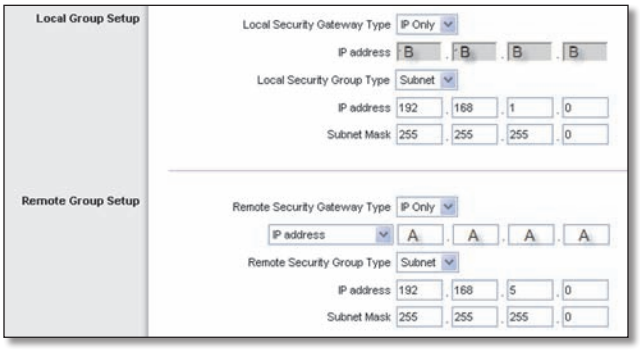
Configuration of the RV082

Follow similar instructions for the RV082.

1. Launch the web browser for a networked computer, designated PC 2.
2. Access the Web-based Utility of the RV082. (Refer to the User Guide of the RV082 for details.)
3. Click the **IPSec VPN** tab.
4. Click the **Gateway to Gateway** tab.
5. Enter a name in the *Tunnel Name* field.

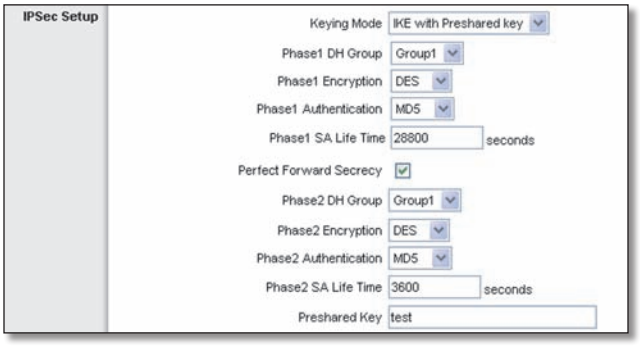
6. For the VPN Tunnel setting, select **Enable**.
7. The WAN IP address (B.B.B.B) of the RV082 will be automatically detected.

   For the Local Security Group Type, select **Subnet**. Enter the RV082's local network settings in the *IP Address* and *Subnet Mask* fields.



RV082 VPN Settings

8. For the Remote Security Gateway Type, select **IP address**. Enter the RVS4000's WAN IP address in the *IP Address* field.
9. For the Remote Security Group Type, select **Subnet**. Enter the RVS4000's local network settings in the *IP Address* and *Subnet Mask* fields.
10. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings. (These should match the settings of the RVS4000.)
11. In the *Preshared Key* field, enter a string for this key, for example, 13572468.



RV082 IPSec Setup Settings

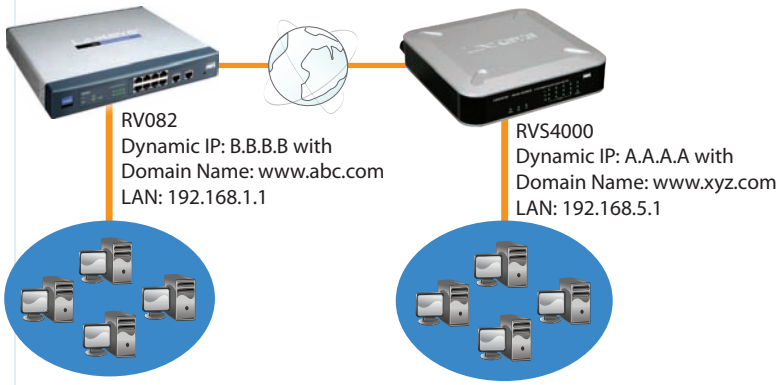
12. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save Settings**.

Configuration of PC 1 and PC 2

Verify that PC 1 and PC 2 can ping each other (refer to Windows Help for more information). If the computers can ping each other, then you know the VPN tunnel is configured correctly.

Configuration when Both Gateways Use Dynamic IP Addresses

This example assumes both Gateways are using dynamic IP addresses. If only the Remote Gateway uses a dynamic IP address, refer to "Configuration when the Remote Gateway Uses a Dynamic IP."



Gateway-to-Gateway IPSec VPN Tunnel - Both Gateways Using Dynamic IP

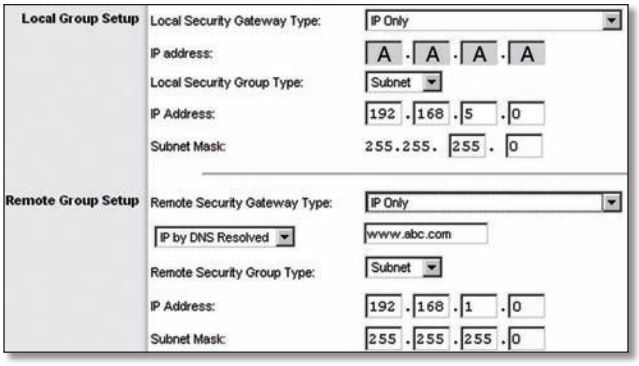
NOTE: Each computer must have a network adapter installed.

Configuration of the RVS4000

Follow these instructions for the first VPN Router, designated RVS4000. The other VPN Router is designated the RV082.

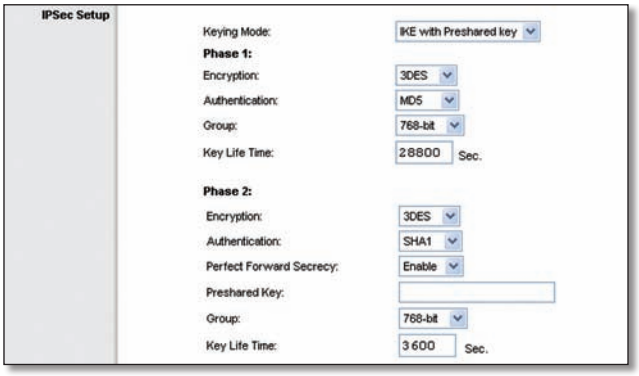
1. Launch the web browser for a networked computer, designated PC 1.
2. Access the web-based utility of the RVS4000. (Refer to "Chapter 5: Setting Up and Configuring the Router" for details.)
3. Click the **VPN** tab.
4. Click **IPSec VPN**.
5. Enter a name in the *Tunnel Name* field.
6. For the IPSec VPN Tunnel setting, select **Enable**.
7. The WAN IP address (A.A.A.A) of the RVS4000 will be automatically detected.

   For the Local Security Group Type, select **Subnet**. Enter the RVS4000's local network settings in the *IP Address* and *Subnet Mask* fields.



RVS4000 IPSec VPN Settings

8. For the Remote Security Gateway Type, select **IP by DNS Resolved**. Enter the RV082's domain name in the field provided.
9. For the Remote Security Group Type, select **Subnet**. Enter the RV082's local network settings in the *IP Address* and *Subnet Mask* fields.
10. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings.
11. In the *Preshared Key* field, enter a string for this key, for example, 13572468.



RVS4000 IPSec Setup Settings

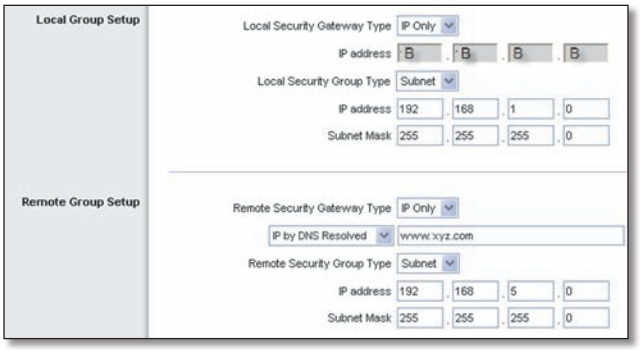
12. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save Settings** and proceed to the next section, "Configuration of the RV082."

Configuration of the RV082

Follow similar instructions for the RV082.

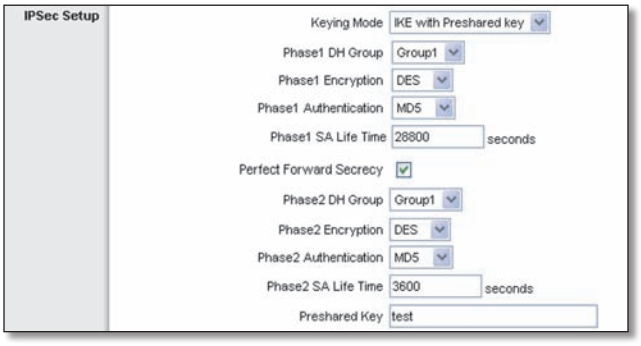
1. Launch the web browser for a networked computer, designated PC 2.
2. Access the Web-based Utility of the RV082. (Refer to the User Guide of the RV082 for details.)
3. Click the **IPSec VPN** tab.
4. Click the **Gateway to Gateway** tab.
5. Enter a name in the *Tunnel Name* field.
6. For the VPN Tunnel setting, select **Enable**.
7. The WAN IP address (B.B.B.B) of the RV082 will be automatically detected.

   For the Local Security Group Type, select **Subnet**. Enter the RV082's local network settings in the *IP Address* and *Subnet Mask* fields.



RV082 VPN Settings

8. For the Remote Security Gateway Type, select **IP by DNS Resolved**. Enter the RVS4000's domain name in the field provided.
9. For the Remote Security Group Type, select **Subnet**. Enter the RVS4000's local network settings in the *IP Address* and *Subnet Mask* fields.
10. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings. (These should match the settings of the RVS4000.)
11. In the *Preshared Key* field, enter a string for this key, for example, 13572468.



RV082 IPSec Setup Settings

12. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save Settings**.

Configuration of PC 1 and PC 2

Verify that PC 1 and PC 2 can ping each other (refer to Windows Help for more information). If the computers can ping each other, then you know the VPN tunnel is configured correctly.

Appendix E: Trend Micro ProtectLink Gateway Service

Overview

The optional Trend Micro ProtectLink Gateway service provides security for your network. It checks e-mail messages, filters website addresses (URLs), and blocks potentially malicious websites. (To purchase a license for this service, contact your Linksys reseller.)

This appendix explains how to use this service.

How to Access the Web-Based Utility

1. For local access of the Router's web-based utility, launch your web browser, and enter the Router's default IP address, **192.168.1.1**, in the *Address* field. Press the **Enter** key.

Address Bar

NOTE: If the Remote Management feature on the *Firewall* > *General* screen has been enabled, then users with administrative privileges can remotely access the web-based utility. Use **http://<WAN IP address of the Router>**, or use **https://<WAN IP address of the Router>** if you have enabled the HTTPS feature.

2. A login screen prompts you for your User name and Password. Enter **admin** in the *User name* field, and enter **admin** in the *Password* field. (You can change the Password on the *Setup* > *Password* screen.) Then click **OK**.

Login Screen

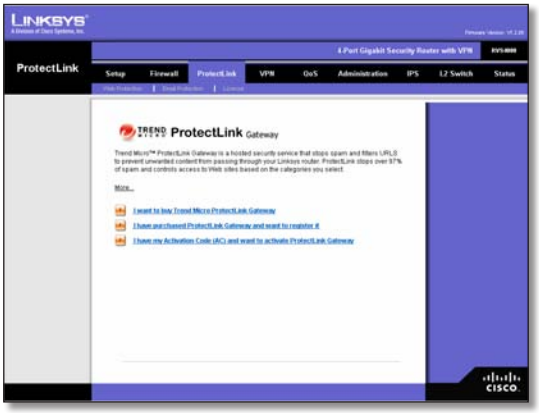
How to Purchase, Register, or Activate the Service

You can purchase, register, or activate the service using the *ProtectLink* screen.

ProtectLink

Click the **ProtectLink** tab to display this screen.

NOTE: If the ProtectLink tab is not displayed, upgrade the Router's firmware. Refer to "Appendix F: Firmware Upgrade" for instructions.



ProtectLink

Follow the instructions for the appropriate option:

- I want to buy Trend Micro ProtectLink.
- I want to register online.
- I want to activate Trend Micro ProtectLink.

I want to buy Trend Micro ProtectLink Gateway. To purchase a license to use this service, click this link. You will be redirected to a list of Linksys resellers on the Linksys website. Then follow the on-screen instructions.

I have purchased ProtectLink Gateway and want to register it. If you already have a license, click this link. You will be redirected to the Trend Micro ProtectLink Gateway website. Then follow the on-screen instructions.

NOTE: To have your e-mail checked, you will need to provide the domain name and IP address of your e-mail server. If you do not know this information, contact your ISP.

I have my Activation Code (AC) and want to activate ProtectLink Gateway. If you have registered, click this link. A wizard begins. Follow the on-screen instructions.

When the wizard is complete, the Web Protection, Email Protection, and License tabs will appear.

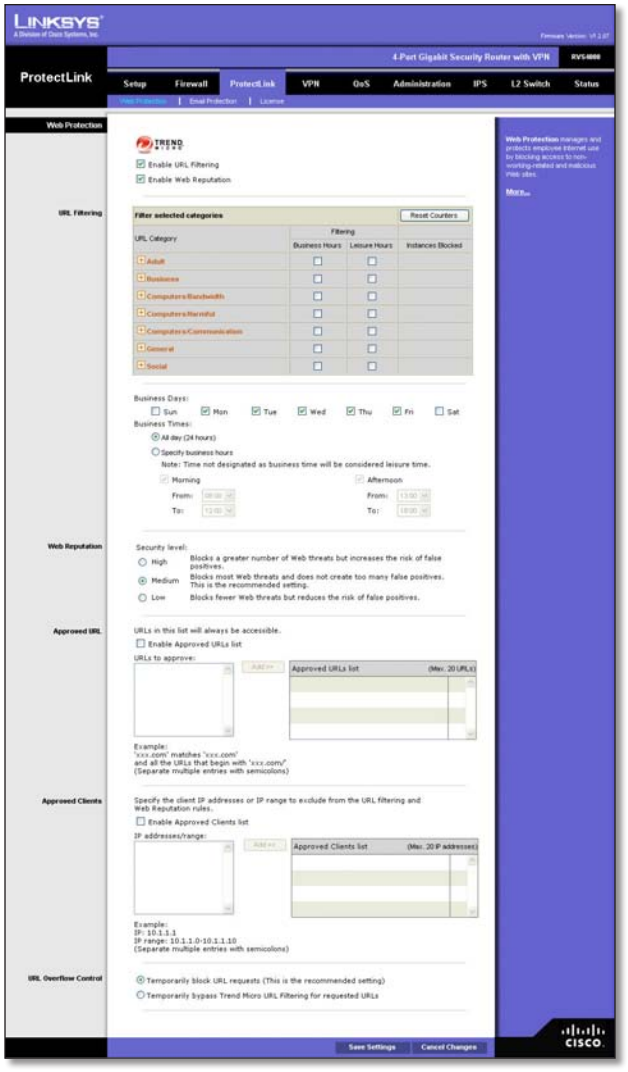
NOTE: If you replace the Router with a new router that supports this service, click **I have my Activation Code (AC) and want to activate ProtectLink Gateway**. Then use your current activation code to transfer your license for the ProtectLink service to the new router.

How to Use the Service

Configure the service to protect your network.

ProtectLink > Web Protection

The Web Protection features are provided by the Router. Configure the website filtering settings on this screen.



ProtectLink > Web Protection

Web Protection

Enable URL Filtering To filter website addresses (URLs), select this option.

Enable Web Reputation To block potentially malicious websites, select this option.

URL Filtering

Reset Counter The Router counts the number of attempted visits to a restricted URL. To reset the counter to zero, click **Reset Counter**.

For each URL category, select the appropriate Filtering option. If you want to filter a sub-category, click **+** to view the sub-categories for each category. Then select the appropriate Filtering option:

Business Hours To filter this URL category during the business hours you have specified, select this option.

Leisure Hours To filter this URL category during non-business hours, select this option.

Instances Blocked The number of attempted visits is displayed.

Business Hour Setting

Business Days Select the appropriate days. The default days are **Mon.** through **Fri.**

Business Times To specify entire days, keep the default, **All day (24 hours)**. To specify hours, select **Specify business hours**. For morning hours, select **Morning**, and then select the appropriate *From* and *To* times. For afternoon hours, select **Afternoon**, and then select the appropriate *From* and *To* times.

Web Reputation

Select the appropriate security level:

High This level blocks a higher number of potentially malicious websites but also increases the risk of false positives. (A false positive is a website that can be trusted but seems potentially malicious.)

Medium This level blocks most potentially malicious websites and does not create too many false positives. The default is **Medium** and is the recommended setting.

Low This level blocks fewer potentially malicious websites and reduces the risk of false positives.

Approved URLs

You can designate up to 20 trusted URLs that will always be accessible.

Enable Approved URL list To set up a list of always accessible URLs, select this option.

URL(s) to approve Enter the trusted URL(s). Separate multiple URLs with semicolons (“**;**”).

Add To add the URLs, click **Add**.

Approved URLs list The trusted URLs are displayed. To delete a URL, click its **trash can** icon.

Approved Clients

You can designate up to 20 trusted clients (local IP addresses) that will always have access to filtered URLs.

Enable Approved Client list To set up a list of trusted clients, select this option.

IP addresses/range Enter the appropriate IP addresses or ranges. Separate multiple URLs with semicolons (“**;**”). For a range of IP addresses, use a hyphen (“**-**”). Example: 10.1.1.0-10.1.1.10.

Add To add the IP addresses or ranges, click **Add**.

Approved Clients list The IP addresses or range of trusted clients are displayed. To delete an IP address or range, click its **trash can** icon.

URL Overflow Control

Specify the behavior you want if there are more URL requests than the service can handle.

Temporarily block URL requests (This is the recommended setting) If there are too many URL requests, the overflow will be held back until they can be processed. This is the default setting.

Temporarily bypass Trend Micro URL verification for requested URLs If there are too many URL requests, the overflow will be allowed without verification.

Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them.

ProtectLink > Email Protection

The Email Protection features are provided by an online service called IMHS, which stands for InterScan™ Messaging Hosted Security. It checks your e-mail messages so spam, viruses, and inappropriate content are filtered out. After you have configured the IMHS settings, your e-mail messages will be checked online before appropriate messages are forwarded to your network.

ProtectLink > Email Protection

Email Protection

NOTE: To have your e-mail checked, you will need to provide the domain name and IP address of your e-mail server. If you do not know this information, contact your ISP.

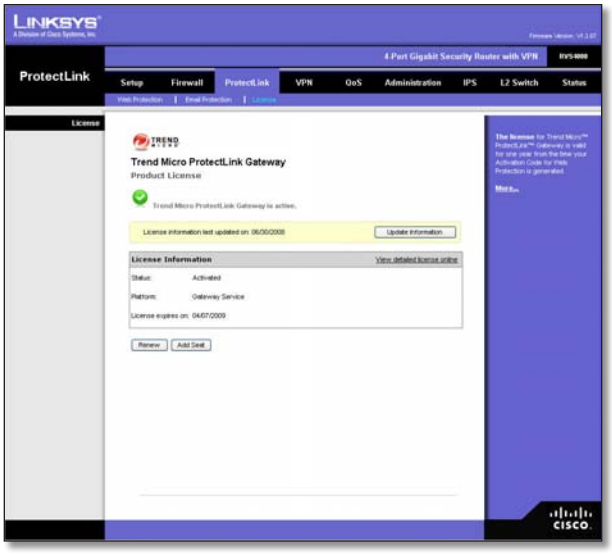
https://us.imhs.trendmicro.com/linksys To set up e-mail protection, click this link. You will be redirected to the Trend Micro ProtectLink Gateway website. Then follow the on-screen instructions.

ProtectLink > License

The license for the Trend Micro ProtectLink Gateway service (Email Protection and Web Protection) is valid for one year from the time the activation code for Web Protection is generated. If you do not provide the necessary information to activate Email Protection during registration, please provide that information as soon as possible because Email Protection and Web Protection will expire at the same time.

NOTE: For example, if you provide the information needed for Email Protection one month after receiving the activation code for Web Protection, then you will receive only 11 months of Email Protection.

On the *License* screen, license information is displayed. Use this screen to renew your license, add seats, or view license information online.



ProtectLink > License

License

Update Information To refresh the license information displayed on-screen, click **Update Information**.

License Information

View detailed license online To view license information online, click this link.

Status The status of your license, Activated or Expired, is displayed.

Platform The platform type, Gateway Service, is automatically displayed.

License expires on The date and time your license expires are displayed.

Renew To renew your license, click **Renew**. Then follow the on-screen instructions.

Add Seats Each seat allows an e-mail account to use Email Protection. To add seats to your license, click **Add Seats**. Then follow the on-screen instructions.

Appendix E

Trend Micro ProtectLink Gateway Service

Appendix F: Specifications

Specifications

Model	RVS4000
Standards	IEEE 802.3, 802.3u, 802.1x, RFC791 (IP Protocol), RFC2460
Ports	Ethernet, Power
Buttons	Reset
Cabling Type	UTP CAT 5
LEDs	Power, Diag, IPS, LAN 1-4, Internet
Operating System	Linux

Performance

NAT Throughput	800 Mb/s

Setup/Config

Web User Interface	Built-in Web UI for easy browser-based configuration (HTTP/HTTPS)

Management

SNMP Version	SNMP version 1, 2c
Event Logging	Local, Syslog, E-mail Alerts
Firmware Upgrade	Firmware Upgradable Through Web Browser
Diagnostics	LEDs for Flash and RAM failure; Ping Test and Traceroute for network diagnostics

Security Features

Access Control	Access Control List (ACL) Capability: MAC-based, IP-based
Firewall	SPI stateful packet inspection firewall
Content Filtering	URL blocking, keyword blocking
IPS (Intrusion Prevention System)	IP Sweep Detection, Application Anomaly Detection (HTTP, FTP, Telnet, RCP), P2P Control, Instant Messenger Control, L3-L4 Protocol (IP, TCP, UDP, ICMP) Normalization, L7 Signature Matching
Signature Update	Manual download from the Web
Secure Management	HTTPS, Username/Password
802.1X	Port-based RADIUS Authentication (EAP-MD5, EAP-PEAP)

QoS

Service-based	Service-based Bandwidth Management supports Rate Control and Priority
Prioritization Types	802.1p, DSCP, and Port-based
Queues	4 queues

Network

VLAN Support	802.1Q VLAN
DHCP	DHCP Server, DHCP Client, DHCP Relay Agent
DNS	DNS Relay, Dynamic DNS (DynDNS, TZO)
NAT	PAT, NAPT
DMZ	One PC in the LAN can be configured as a DMZ Host

VPN

	5 QuickVPN Tunnels for remote client access; 5 IPSec Gateway-to-Gateway Tunnels for branch office connectivity; 3DES Encryption; MD5/SHA1 Authentication; IPSec NAT-T; VPN Passthrough of PPTP, L2TP, IPSec

Routing

	Static and RIP v1, v2 Inter-VLAN Routing

Layer 2

VLAN	Supports four 802.1Q VLANs
Port Mirroring	One of the five WAN/LAN ports can be mirrored to a selected LAN port
RSTP	Supports Rapid Spanning Tree Protocol for loop detection and faster reconfiguration

Environmental

Dimensions W x H x D	6.69" x 1.61" x 6.69" (170 x 41 x 170 mm)
Unit Weight	0.84 lb (0.38 kg)
Power	12V 1A
Certification	FCC Class B, CE, ICES-003
Operating Temp.	32 to 104°F (0 to 40°C)
Storage Temp.	-4 to 158°F (-20 to 70°C)
Operating Humidity	10 to 85% Noncondensing
Storage Humidity	5 to 90% Noncondensing

Specifications are subject to change without notice.

Appendix G: Warranty Information

Linksys warrants this Linksys hardware product against defects in materials and workmanship under normal use for the Warranty Period, which begins on the date of purchase by the original end-user purchaser and lasts for the period specified for this product at **www.linksys.com/warranty**. The internet URL address and the web pages referred to herein may be updated by Linksys from time to time; the version in effect at the date of purchase shall apply.

This limited warranty is non-transferable and extends only to the original end-user purchaser. Your exclusive remedy and Linksys' entire liability under this limited warranty will be for Linksys, at its option, to (a) repair the product with new or refurbished parts, (b) replace the product with a reasonably available equivalent new or refurbished Linksys product, or (c) refund the purchase price of the product less any rebates. Any repaired or replacement products will be warranted for the remainder of the original Warranty Period or thirty (30) days, whichever is longer. All products and parts that are replaced become the property of Linksys.

Exclusions and Limitations

This limited warranty does not apply if: (a) the product assembly seal has been removed or damaged, (b) the product has been altered or modified, except by Linksys, (c) the product damage was caused by use with non-Linksys products, (d) the product has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, (e) the product has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, (f) the serial number on the Product has been altered, defaced, or removed, or (g) the product is supplied or licensed for beta, evaluation, testing or demonstration purposes for which Linksys does not charge a purchase price or license fee.

ALL SOFTWARE PROVIDED BY LINKSYS WITH THE PRODUCT, WHETHER FACTORY LOADED ON THE PRODUCT OR CONTAINED ON MEDIA ACCOMPANYING THE PRODUCT, IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. Without limiting the foregoing, Linksys does not warrant that the operation of the product or software will be uninterrupted or error free. Also, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the product, software or any equipment, system or network on which the product or software is used will be free of vulnerability to intrusion or attack. The product may include or be bundled with third party software or service offerings. This limited warranty shall not apply to such third party software or service offerings. This limited warranty does not guarantee any continued availability of a third party's service for which this product's use or operation may require.

TO THE EXTENT NOT PROHIBITED BY LAW, ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary by jurisdiction.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this limited warranty fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Obtaining Warranty Service

If you have a question about your product or experience a problem with it, please go to **www.linksys.com/support** where you will find a variety of online support tools and information to assist you with your product. If the product proves defective during the Warranty Period, contact the Value Added Reseller (VAR) from whom you purchased the product or Linksys Technical Support for instructions on how to obtain warranty service. The telephone number for Linksys Technical Support in your area can be found in the product User Guide and at **www.linksys.com**. Have your product serial number and proof of purchase on hand when calling. A DATED PROOF OF ORIGINAL PURCHASE IS REQUIRED TO PROCESS WARRANTY CLAIMS. If you are requested to return your product, you will be given a Return Materials Authorization (RMA) number. You are responsible for properly packaging and shipping your product to Linksys at your cost and risk. You must include the RMA number and a copy of your dated proof of

original purchase when returning your product. Products received without a RMA number and dated proof of original purchase will be rejected. Do not include any other items with the product you are returning to Linksys. Defective product covered by this limited warranty will be repaired or replaced and returned to you without charge. Customers outside of the United States of America and Canada are responsible for all shipping and handling charges, custom duties, VAT and other associated taxes and charges. Repairs or replacements not covered under this limited warranty will be subject to charge at Linksys' then-current rates.

Technical Support

This limited warranty is neither a service nor a support contract. Information about Linksys' current technical support offerings and policies (including any fees for support services) can be found at: **www.linksys.com/support**.

This limited warranty is governed by the laws of the jurisdiction in which the Product was purchased by you.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.

Appendix H: Regulatory Information

FCC Statement

This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

Safety Notices

- Caution: To reduce the risk of fire, use only No.26 AWG or larger telecommunication line cord.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

WARNING: This product contains lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. Wash hands after handling.

Industry Canada Statement

This Class B digital apparatus complies with Canadian ICES-003.

Operation is subject to the following two conditions:

1. This device may not cause interference and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Avis d'Industrie Canada

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Le fonctionnement est soumis aux conditions suivantes :

1. Ce périphérique ne doit pas causer d'interférences;
2. Ce périphérique doit accepter toutes les interférences reçues, y compris celles qui risquent d'entraîner un fonctionnement indésirable.

User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)

This document contains important information for users with regards to the proper disposal and recycling of Linksys products. Consumers are required to comply with this notice for all electronic products bearing the following symbol:

English - Environmental Information for Customers in the European Union

European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

Български (Bulgarian) - Информация относно опазването на околната среда за потребители в Европейския съюз

Европейска директива 2002/96/ЕС изисква уредите, носещи този символ върху изделието и/или опаковката му, да не се изхвърля т с несортирани битови отпадъци. Символът обозначава, че изделието трябва да се изхвърля отделно от сметосъбирането на обикновените битови отпадъци. Ваша е отговорността този и другите електрически и електронни уреди да се изхвърлят в предварително определени от държавните или общински органи специализирани пунктове за събиране. Правилното изхвърляне и рециклиране ще спомогнат да се предотвратят евентуални вредни за околната среда и здравето на населението последствия. За по-подробна информация относно изхвърлянето на вашите стари уреди се обърнете към местните власти, службите за сметосъбиране или магазина, от който сте закупили уреда.

Ceština (Czech) - Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie

Evropská směrnice 2002/96/ES zakazuje, aby zařízení označené tímto symbolem na produktu anebo na obalu bylo likvidováno s netříděným komunálním odpadem. Tento symbol udává, že daný produkt musí být likvidován odděleně od běžného komunálního odpadu. Odpovídáte za likvidaci tohoto produktu a dalších elektrických a elektronických zařízení prostřednictvím určených sběrných míst stanovených vládou nebo místními úřady. Správná likvidace a recyklace pomáhá předcházet potenciálním negativním dopadům na životní prostředí a lidské zdraví. Podrobnější informace o likvidaci starého vybavení si laskavě vyžádejte od místních úřadů, podniku zabývajícího se likvidací komunálních odpadů nebo obchodu, kde jste produkt zakoupili.

Dansk (Danish) - Miljøinformation for kunder i EU

EU-direktiv 2002/96/EF kræver, at udstyr der bærer dette symbol på produktet og/eller emballagen ikke må bortskaffes som usorteret kommunalt affald. Symbolet betyder, at dette produkt skal bortskaffes adskilt fra det almindelige husholdningsaffald. Det er dit ansvar at bortskaffe dette og andet elektrisk og elektronisk udstyr via bestemte indsamlingssteder udpeget af staten eller de lokale myndigheder. Korrekt bortskaffelse og genvinding vil hjælpe med til at undgå mulige skader for miljøet og menneskers sundhed. Kontakt venligst de lokale myndigheder, renovationstjenesten eller den butik, hvor du har købt produktet, angående mere detaljeret information om bortskaffelse af dit gamle udstyr.

Deutsch (German) - Umweltinformation für Kunden innerhalb der Europäischen Union

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist, nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

Eesti (Estonian) - Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele

Euroopa Liidu direktiivi 2002/96/EÜ nõuete kohaselt on seadmeid, millel on tootel või pakendil käesolev sümbol, keelatud kõrvaldada koos sorteerimata olmejäätmetega. See sümbol näitab, et toode tuleks kõrvaldada eraldi tavalistest olmejäätmevoogudest. Olete kohustatud kõrvaldama käesoleva ja ka muud elektri- ja elektroonikaseadmed riigi või kohalike ametiasutuste poolt ette nähtud kogumispunktide kaudu. Seadmete korrektne kõrvaldamine ja ringlussevõtt aitab vältida võimalikke negatiivseid tagajärgi keskkonnale ning inimeste tervisele. Vanade seadmete kõrvaldamise kohta täpsema informatsiooni saamiseks võtke palun ühendust kohalike ametiasutustega, jäätmekäitlusfirmaga või kauplusega, kust te toote ostsite.

Español (Spanish) - Información medioambiental para clientes de la Unión Europea

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.

ξλληνικά (Greek) - Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι ο εξοπλισμός ο οποίος φέρει αυτό το σύμβολο στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινοτικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν θα πρέπει να απορρίπτεται ξεχωριστά από τα συνήθη οικιακά απορρίμματα. Είστε υπεύθυνος για την απόρριψη του παρόντος και άλλου ηλεκτρικού και ηλεκτρονικού εξοπλισμού μέσω των καθορισμένων εγκαταστάσεων συγκέντρωσης απορριμμάτων οι οποίες παρέχονται από το κράτος ή τις αρμόδιες τοπικές αρχές. Η σωστή απόρριψη και ανακύκλωση συμβάλλει στην πρόληψη πιθανών αρνητικών συνεπειών για το περιβάλλον και την υγεία. Για περισσότερες πληροφορίες σχετικά με την απόρριψη του παλιού σας εξοπλισμού, παρακαλώ επικοινωνήστε με τις τοπικές αρχές, τις υπηρεσίες απόρριψης ή το κατάστημα από το οποίο αγοράσατε το προϊόν.

Français (French) - Informations environnementales pour les clients de l'Union européenne

La directive européenne 2002/96/CE exige que l'équipement sur lequel est apposé ce symbole sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L'élimination et le recyclage en bonne et due forme ont pour but de lutter contre l'impact néfaste potentiel de ce type de produits sur l'environnement et la santé publique. Pour plus d'informations sur le mode d'élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l'endroit où vous avez acheté le produit.

Italiano (Italian) - Informazioni relative all'ambiente per i clienti residenti nell'Unione Europea

La direttiva europea 2002/96/EC richiede che le apparecchiature contrassegnate con questo simbolo sul prodotto e/o sull'imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche ed elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l'ambiente e per la salute dell'essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.

Latviešu valoda (Latvian) - Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

Direktīvā 2002/96/EK ir prasība, ka aprīkojumu, kam pievienota zīme uz paša izstrādājuma vai uz tā iesaiņojuma, nedrīkst izmest nešķirotā veidā kopā ar komunālajiem atkritumiem (tiem, ko rada vietēji iedzīvotāji un uzņēmumi). Šī zīme nozīmē to, ka šī ierīce ir jāizmet atkritumos tā, lai tā nenonāktu kopā ar parastiem mājsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskas un elektroniskas ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmešana atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākas ziņas par novecojuša aprīkojuma izmešanu atkritumos jūs varat saņemt vietējā pašvaldībā, atkritumu savākšanas dienestā, kā arī veikalā, kur iegādājāties šo izstrādājumu.

Lietuvškai (Lithuanian) - Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir kurios pakuotė yra pažymėta šiuo simboliu (įveskite simbolį), negalima šalinti kartu su nerūšiuotomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminį reikia šalinti atskirai nuo bendro buitinių atliekų srauto. Jūs privalote užtikrinti, kad ši ir kita elektros ar elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemas. Tinkamai šalinant ir perdirbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie jūsų senos įrangos šalinimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduotuvės, kuriose įsigijote tą gaminį.

Malti (Maltese) - Informazzjoni Ambjentali għal Klijenti fl-Unjoni Ewropea

Id-Direttiva Ewropea 2002/96/KE titlob li t-tagħmir li jkun fih is-simbolu fuq il-prodott u/jew fuq l-ippakkjar ma jistax jintrema ma' skart muniċipali li ma ġiex isseparat. Is-simbolu jindika li dan il-prodott għandu jintrema separatament minn ma' l-iskart domestiku regolari. Hija responsabbiltà tiegħek li tarmi dan it-tagħmir u kull tagħmir ieħor ta' l-elettriku u elettroniku permezz ta' faċilitajiet ta' ġbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riċiklaġġ jgħin jipprevjeni konsegwenzi negattivi potenzjali għall-ambjent u għas-saħħa tal-bniedem. Għal aktar informazzjoni dettaljata dwar ir-rimi tat-tagħmir antik tiegħek, jekk jogħġbok ikkuntattja lill-awtoritajiet lokali tiegħek, is-servizzi għar-rimi ta' l-iskart, jew il-ħanut minn fejn xtrajt il-prodott.

Magyar (Hungarian) - Környezetvédelmi információ az európai uniós vásárlók számára

A 2002/96/EC számú európai uniós irányelv megkívánja, hogy azokat a termékeket, amelyeken, és/vagy amelyek csomagolásán az alábbi címke megjelenik, tilos a többi szelektálatlan lakossági hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékelszállítási rendszerektõl elkülönített eljárást kell alkalmazni. Az Ön felelõssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtõredszereken keresztül számolja fel. A megfelelõ hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelõzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgálattal, vagy azzal üzlettel, ahol a terméket vásárolta.

Nederlands (Dutch) - Milieu-informatie voor klanten in de Europese Unie

De Europese Richtlijn 2002/96/EC schrijft voor dat apparatuur die is voorzien van dit symbool op het product of de verpakking, niet mag worden ingezameld met niet-gescheiden huishoudelijk afval. Dit symbool geeft aan dat het product apart moet worden ingezameld. U bent zelf verantwoordelijk voor de vernietiging van deze en andere elektrische en elektronische apparatuur via de daarvoor door de landelijke of plaatselijke overheid aangewezen inzamelingskanalen. De juiste vernietiging en recycling van deze apparatuur voorkomt mogelijke negatieve gevolgen voor het milieu en de gezondheid. Voor meer informatie over het vernietigen van uw oude apparatuur neemt u contact op met de plaatselijke autoriteiten of afvalverwerkingsdienst, of met de winkel waar u het product hebt aangeschaft.

Norsk (Norwegian) - Miljøinformasjon for kunder i EU

EU-direktiv 2002/96/EF krever at utstyr med følgende symbol avbildet på produktet og/eller pakningen, ikke må kastes sammen med usortert avfall. Symbolet indikerer at dette produktet skal håndteres atskilt fra ordinær avfallsinnsamling for husholdningsavfall. Det er ditt ansvar å kvitte deg med dette produktet og annet elektrisk og elektronisk avfall via egne innsamlingsordninger slik myndighetene eller kommunene bestemmer. Korrekt avfallshåndtering og gjenvinning vil være med på å forhindre mulige negative konsekvenser for miljø og helse. For nærmere informasjon om håndtering av det kasserte utstyret ditt, kan du ta kontakt med kommunen, en innsamlingsstasjon for avfall eller butikken der du kjøpte produktet.

Polski (Polish) - Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w punktach odbioru wyznaczonych przez władze krajowe lub lokalne. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu, prosimy zwrócić się do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.

Português (Portuguese) - Informação ambiental para clientes da União Europeia

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É da sua responsabilidade eliminar este e qualquer outro equipamento eléctrico e electrónico através das instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem correctas ajudarão a prevenir as consequências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o seu equipamento antigo, contacte as autoridades locais, os serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

Română (Romanian) - Informații de mediu pentru clienții din Uniunea Europeană

Directiva europeană 2002/96/CE impune ca echipamentele care prezintă acest simbol pe produs şi/sau pe ambalajul acestuia să nu fie casate împreună cu gunoiul menajer municipal. Simbolul indică faptul că acest produs trebuie să fie casat separat de gunoiul menajer obişnuit. Este responsabilitatea dvs. să casați acest produs şi alte echipamente electrice şi electronice prin intermediul unităților de colectare special desemnate de guvern sau de autoritățile locale. Casarea şi reciclarea corecte vor ajuta la prevenirea potențialelor consecințe negative asupra sănătății mediului şi a oamenilor. Pentru mai multe informații detaliate cu privire la casarea acestui echipament vechi, contactați autoritățile locale, serviciul de salubrizare sau magazinul de la care ați achiziționat produsul.

Slovenčina (Slovak) - Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

Podľa európskej smernice 2002/96/ES zariadenie s týmto symbolom na produkte a/alebo jeho balení nesmie byť likvidované spolu s netriedeným komunálnym odpadom. Symbol znamená, že produkt by sa mal likvidovať oddelene od bežného odpadu z domácností. Je vašou povinnosťou likvidovať toto i ostatné elektrické a elektronické zariadenia prostredníctvom špecializovaných zberných zariadení určených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia pomôže zabrániť prípadným negatívnym dopadom na životné prostredie a zdravie ľudí. Ak máte záujem o podrobnejšie informácie o likvidácii starého zariadenia, obráťte sa, prosím, na miestne orgány, organizácie zaoberajúce sa likvidáciou odpadov alebo obchod, v ktorom ste si produkt zakúpili.

Slovenčina (Slovene) - Okoljske informacije za stranke v Evropski uniji

Evropska direktiva 2002/96/EC prepoveduje odlaganje opreme, označene s tem simbolom – na izdelku in/ali na embalaži – med običajne, nerazvrščene odpadke. Ta simbol opozarja, da je treba izdelek odvreči ločeno od preostalih gospodinjskih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbirališča, ki jih določijo državne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste preprečili morebitne škodljive vplive na okolje in zdravje ljudi. Če želite izvedeti več o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.

Suomi (Finnish) - Ympäristöä koskevia tietoja EU-alueen asiakkaille

EU-direktiivi 2002/96/EY edellyttää, että jos laitteistossa on tämä symboli itse tuotteessa ja/tai sen pakkauksessa, laitteistoa ei saa hävittää lajittelemattoman yhdyskuntajätteen mukana. Symboli merkitsee sitä, että tämä tuote on hävitettävä erillään tavallisesta kotitalousjätteestä. Sinun vastuullasi on hävittää tämä elektroniikkatuote ja muut vastaavat elektroniikkatuotteet viemällä tuote tai tuotteet viranomaisten määräämään keräyspisteeseen. Laitteiston oikea hävittäminen estää mahdolliset kielteiset vaikutukset ympäristöön ja ihmisten terveyteen. Lisätietoja vanhan laitteiston oikeasta hävitystavasta saa paikallisilta viranomaisilta, jätteenhävityspalvelusta tai siitä myymälästä, josta ostit tuotteen.

Svenska (Swedish) - Miljöinformation för kunder i Europeiska unionen

Det europeiska direktivet 2002/96/EC kräver att utrustning med denna symbol på produkten och/eller förpackningen inte får kastas med osorterat kommunalt avfall. Symbolen visar att denna produkt bör kastas efter att den avskiljts från vanligt hushållsavfall. Det faller på ditt ansvar att kasta denna och annan elektrisk och elektronisk utrustning på fastställda insamlingsplatser utsedda av regeringen eller lokala myndigheter. Korrekt kassering och återvinning skyddar mot eventuella negativa konsekvenser för miljön och personhälsa. För mer detaljerad information om kassering av din gamla utrustning kontaktar du dina lokala myndigheter, avfallshanteringen eller butiken där du köpte produkten.

WEB: For additional information, please visit **www.linksys.com**

Appendix I: Software License Agreement

Software in Linksys Products:

This product from Cisco-Linksys LLC or from one of its affiliates Cisco Systems-Linksys (Asia) Pte Ltd. or Cisco-Linksys K.K. ("Linksys") contains software (including firmware) originating from Linksys and its suppliers and may also contain software from the open source community. Any software originating from Linksys and its suppliers is licensed under the Linksys Software License Agreement contained at Schedule 1 below. You may also be prompted to review and accept that Linksys Software License Agreement upon installation of the software.

Any software from the open source community is licensed under the specific license terms applicable to that software made available by Linksys at www.linksys.com/gpl or as provided for in Schedules 2 and 3 below.

Where such specific license terms entitle you to the source code of such software, that source code is upon request available at cost from Linksys for at least three years from the purchase date of this product and may also be available for download from www.linksys.com/gpl. For detailed license terms and additional information on open source software in Linksys products please look at the Linksys public web site at: www.linksys.com/gpl/ or Schedule 2 below as applicable.

BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THE SOFTWARE LICENSE AGREEMENTS BELOW. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN UNUSED SOFTWARE (OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, THE UNUSED PRODUCT) FOR A FULL REFUND UP TO 30 DAYS AFTER ORIGINAL PURCHASE, SUBJECT TO THE RETURN PROCESS AND POLICIES OF THE PARTY FROM WHICH YOU PURCHASED SUCH PRODUCT OR SOFTWARE.

Software Licenses:

The software Licenses applicable to software from Linksys are made available at the Linksys public web site at: www.linksys.com and www.linksys.com/gpl/ respectively. For your convenience of reference, a copy of the Linksys Software License Agreement and the main open source code licenses used by Linksys in its products are contained in the Schedules below.

Schedule 1 Linksys Software License Agreement

THIS LICENSE AGREEMENT IS BETWEEN YOU AND CISCO-LINKSYS LLC OR ONE OF ITS AFFILIATES CISCO SYSTEMS-LINKSYS (ASIA) PTE LTD. OR CISCO-LINKSYS K.K. ("LINKSYS") LICENSING THE SOFTWARE INSTEAD OF CISCO-LINKSYS LLC. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN UNUSED SOFTWARE (OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, THE UNUSED PRODUCT) FOR A FULL REFUND UP TO 30 DAYS AFTER ORIGINAL PURCHASE, SUBJECT TO THE RETURN PROCESS AND POLICIES OF THE PARTY FROM WHICH YOU PURCHASED SUCH PRODUCT OR SOFTWARE.

License. Subject to the terms and conditions of this Agreement, Linksys grants the original end user purchaser of the Linksys product containing the Software ("You") a nonexclusive license to use the Software solely as embedded in or (where authorized in the applicable documentation) for communication with such product. This license may not be sublicensed, and is not transferable except to a person or entity to which you transfer ownership of the complete Linksys product containing the Software, provided you permanently transfer all rights under this Agreement and do not retain any full or partial copies of the Software, and the recipient agrees to the terms of this Agreement.

"Software" includes, and this Agreement will apply to (a) the software of Linksys or its suppliers provided in or with the applicable Linksys product, and (b) any upgrades, updates, bug fixes or modified versions ("Upgrades") or backup copies of the Software supplied to You by Linksys or an authorized reseller, provided you already hold a valid license to the original software and have paid any applicable fee for the Upgrade.

Protection of Information. The Software and documentation contain trade secrets and/or copyrighted materials of Linksys or its suppliers. You will not copy or modify the Software or decompile, decrypt, reverse engineer or disassemble the Software (except to the extent expressly permitted by law notwithstanding this provision), and You will not disclose or make available such trade secrets or copyrighted material in any form to any third party. Title to and ownership of the Software and documentation and any portion thereof, will remain solely with Linksys or its suppliers.

Collection and Processing of Information. You agree that Linksys and/or its affiliates may, from time to time, collect and process information about your Linksys product and/or the Software and/or your use of either in order (i) to enable Linksys to offer you Upgrades; (ii) to ensure that

your Linksys product and/or the Software is being used in accordance with the terms of this Agreement; (iii) to provide improvements to the way Linksys delivers technology to you and to other Linksys customers; (iv) to enable Linksys to comply with the terms of any agreements it has with any third parties regarding your Linksys product and/or Software and/or (v) to enable Linksys to comply with all applicable laws and/or regulations, or the requirements of any regulatory authority or government agency. Linksys and/ or its affiliates may collect and process this information provided that it does not identify you personally. Your use of your Linksys product and/or the Software constitutes this consent by you to Linksys and/ or its affiliates' collection and use of such information and, for EEA customers, to the transfer of such information to a location outside the EEA.

Software Upgrades etc. If the Software enables you to receive Upgrades, you may elect at any time to receive these Upgrades either automatically or manually. If you elect to receive Upgrades manually or you otherwise elect not to receive or be notified of any Upgrades, you may expose your Linksys product and/or the Software to serious security threats and/or some features within your Linksys product and/or Software may become inaccessible. There may be circumstances where we apply an Upgrade automatically in order to comply with changes in legislation, legal or regulatory requirements or as a result of requirements to comply with the terms of any agreements Linksys has with any third parties regarding your Linksys product and/or the Software. You will always be notified of any Upgrades being delivered to you. The terms of this license will apply to any such Upgrade unless the Upgrade in question is accompanied by a separate license, in which event the terms of that license will apply.

Open Source Software. The GPL or other open source code incorporated into the Software and the open source license for such source code are available for free download at http://www.linksys.com/gpl. If You would like a copy of the GPL or other open source code in this Software on a CD, Linksys will mail to You a CD with such code for $9.99 plus the cost of shipping, upon request.

Term and Termination. You may terminate this License at any time by destroying all copies of the Software and documentation. Your rights under this License will terminate immediately without notice from Linksys if You fail to comply with any provision of this Agreement.

Limited Warranty. The warranty terms and period specified in the applicable Linksys Product User Guide shall also apply to the Software.

Disclaimer of Liabilities. IN NO EVENT WILL LINKSYS OR ITS SUPPLIERS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF CAUSE (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

Export. Software, including technical data, may be subject to U.S. export control laws and regulations and/or export or import regulations in other countries. You agree to comply strictly with all such laws and regulations.

U.S. Government Users. The Software and documentation qualify as "commercial items" as defined at 48 C.F.R. 2.101 and 48 C.F.R. 12.212. All Government users acquire the Software and documentation with only those rights herein that apply to non-governmental customers.

General Terms. This Agreement will be governed by and construed in accordance with the laws of the State of California, without reference to conflict of laws principles. The United Nations Convention on Contracts for the International Sale of Goods will not apply. If any portion of this Agreement is found to be void or unenforceable, the remaining provisions will remain in full force and effect. This Agreement constitutes the entire agreement between the parties with respect to the Software and supersedes any conflicting or additional terms contained in any purchase order or elsewhere.

END OF SCHEDULE 1

Schedule 2

If this Linksys product contains open source software licensed under Version 2 of the "GNU General Public License" then the license terms below in this Schedule 2 will apply to that open source software. The license terms below in this Schedule 2 are from the public web site at http://www.gnu.org/copyleft/gpl.html.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this

License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

END OF SCHEDULE 2

Schedule 3

If this Linksys product contains open source software licensed under the OpenSSL license then the license terms below in this Schedule 3 will apply to that open source software. The license terms below in this Schedule 3 are from the public web site at http://www.openssl.org/source/license.html

---

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/* ====================================

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL

THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

END OF SCHEDULE 3s

Appendix J: Contact Information

Linksys Contact Information	
Website	http://www.linksys.com
Support Site	http://www.linksys.com/support
FTP Site	ftp.linksys.com
Advice Line	800-546-5797 (LINKSYS)
Support	800-326-7114
RMA (Return Merchandise Authorization)	http://www.linksys.com/warranty

NOTE: Details on warranty and RMA issues can be found in the Warranty section of this Guide.